IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of
Inventor(s): Saori NISHIMURA

Appln. No.: Series Code ↑ | ↑ Serial No.

Group Art Unit: Not Yet Assigned

Filed: Herewith

Examiner: Not Yet Assigned

Title: IC CARD TERMINAL UNIT AND IC CARD DUPLICATION METHOD

Atty. Dkt. P 282732 | T4IA-01S0063-1
M# | Client Ref

Date: October 15, 2001

SUBMISSION OF PRIORITY DOCUMENT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 55

Hon. Asst Commissioner of Patents
Washington, D.C. 20231

Sir:

Please accept the enclosed certified copy(ies) of the respective foreign application(s) listed below for which benefit under 35 U.S.C. 119/365 has been previously claimed in the subject application and if not is hereby claimed.

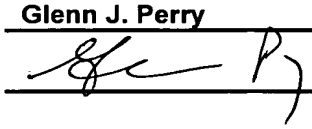
Application No.	Country of Origin	Filed
2001-043630	JAPAN	February 20, 2001

Respectfully submitted,

Pillsbury Winthrop LLP
Intellectual Property Group

1600 Tysons Boulevard
McLean, VA 22102
Tel: (703) 905-2000

By Atty: Glenn J. Perry **Reg. No.** 28458

Sig: 

Fax: (703) 905-2500
Tel: (703) 905-2161

Atty/Sec: gjp/vaw

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００１年 ２月２０日

出 願 番 号
Application Number: 特願２００１－０４３６３０

出 願 人
Applicant (s): 株式会社東芝

２００１年 ３月１６日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号 出証特２００１－３０２０９６２

【書類名】　特許願

【整理番号】　A000007563

【提出日】　平成13年 2月20日

【あて先】　特許庁長官　殿

【国際特許分類】　G06K 17/00

【発明の名称】　ＩＣカード、ＩＣカード端末装置およびＩＣカード複製方法

【請求項の数】　13

【発明者】

【住所又は居所】　神奈川県川崎市幸区柳町７０番地　株式会社東芝柳町事業所内

【氏名】　西村　佐織

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ＩＣカード、ＩＣカード端末装置およびＩＣカード複製方法

【特許請求の範囲】

【請求項１】　外部装置との間でデータを通信する通信手段と、

少なくともデータを暗号化あるいは復号化するための第１の鍵を記憶している記憶手段と、

前記通信手段を介して受信されたデータが鍵設定命令である場合、この鍵設定命令に付加された第２の鍵を前記記憶手段に記憶せしめる鍵設定手段と、

前記通信手段を介して受信されたデータが鍵取出命令である場合、前記鍵設定手段により前記記憶手段に記憶された第２の鍵で前記記憶手段内の第１の鍵を暗号化し、この暗号化した第１の鍵を前記通信手段を介して外部へ出力する鍵出力手段と、

を具備したことを特徴とするＩＣカード。

【請求項２】　前記記憶手段内の第１の鍵は、前記通信手段を介して外部から入力された鍵生成命令に基づき該ＩＣカード内で生成されたものであることを特徴とする請求項１記載のＩＣカード。

【請求項３】　前記記憶手段内の第１の鍵は、外部で生成され、前記通信手段を介して外部から入力されたものであることを特徴とする請求項１記載のＩＣカード。

【請求項４】　前記鍵設定命令は、該ＩＣカードの発行者によって前記通信手段を介して外部から入力されたものであることを特徴とする請求項１記載のＩＣカード。

【請求項５】　前記鍵設定命令は、該ＩＣカードの所持者によって前記通信手段を介して外部から入力されたものであることを特徴とする請求項１記載のＩＣカード。

【請求項６】　一方には少なくともデータを暗号化あるいは復号化するための鍵が記憶され、他方には該鍵が記憶されていない２つのＩＣカードとの間でデータを通信する通信手段と、

前記鍵が記憶された一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内の鍵を前記通信手段を介して取出す鍵取出手段と、

前記鍵が記憶されていない他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該鍵を前記他方のＩＣカード内に記憶せしめる暗号鍵設定手段と、

を具備したことを特徴とするＩＣカード端末装置。

【請求項７】　２つのＩＣカードとの間でデータを通信する通信手段と、

前記２つのＩＣカードに対し、第１の鍵を暗号化あるいは復号化するための第２の鍵を付加した鍵設定命令を前記通信手段を介して送信することにより、該第２の鍵を前記２つのＩＣカード内にそれぞれ記憶せしめる第１の鍵設定手段と、

この第１の鍵設定手段による前記第２の鍵の設定が正常に終了したことを確認する確認手段と、

この確認手段により第２の鍵の設定が正常に終了したことが確認されると、前記２つのＩＣカードのうち一方のＩＣカードに対し鍵生成命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内においてデータを暗号化あるいは復号化するための前記第１の鍵を生成せしめる鍵生成手段と、

この鍵生成手段により第１の鍵を生成させた前記一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内で生成された第１の鍵を前記通信手段を介して取出す鍵取出手段と、

前記２つのＩＣカードのうち他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した第１の鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該第１の鍵を前記他方のＩＣカード内に記憶せしめる第２の鍵設定手段と、

を具備したことを特徴とするＩＣカード端末装置。

【請求項８】　少なくともデータを暗号化あるいは復号化するための鍵が記憶されている被複製用の第１のＩＣカードと、複製用の第２のＩＣカードと、これら第１、第２のＩＣカードを取扱う端末装置とを有し、

前記端末装置から前記第１のＩＣカードに対し鍵取出命令を送信する第１のステップと、

前記第１のＩＣカードにおいて、前記端末装置から送信された鍵取出命令を受信し、前記鍵を前記端末装置に対し送信する第２のステップと、

前記端末装置において、前記第１のＩＣカードから送信された鍵を受信し、この受信した鍵を付加した暗号鍵設定命令を前記第２のＩＣカードに対し送信する第３のステップと、

前記第２のＩＣカードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された鍵を記憶する第４のステップと、

を具備したことを特徴とするＩＣカード複製方法。

【請求項９】　前記第１のＩＣカードに記憶されているデータを暗号化あるいは復号化するための鍵は、前記端末装置から入力された鍵生成命令に基づき該第１のＩＣカード内で生成されたものであることを特徴とする請求項８記載のＩＣカード複製方法。

【請求項１０】　前記第１のＩＣカードに記憶されているデータを暗号化あるいは復号化するための鍵は、外部で生成され、前記端末装置を介して入力されたものであることを特徴とする請求項８記載のＩＣカード複製方法。

【請求項１１】　少なくともデータを暗号化あるいは復号化するための第１の鍵が記憶されている被複製用の第１のＩＣカードと、複製用の第２のＩＣカードと、これら第１、第２のＩＣカードを取扱う端末装置とを有し、

前記端末装置から前記第１、第２のＩＣカードに対し、前記第１の鍵を暗号化あるいは復号化するための第２の鍵を付加した鍵設定命令を送信する第１のステップと、

前記第１、第２のＩＣカードにおいて、前記端末装置から送信された鍵設定命令を受信し、その鍵設定命令に付加された第２の鍵をそれぞれ記憶する第２のステップと、

前記端末装置から前記第１のＩＣカードに対し鍵取出命令を送信する第３のステップと、

前記第１のＩＣカードにおいて、前記端末装置から送信された鍵取出命令を受

信し、前記第２のステップで記憶された第２の鍵により前記第１の鍵を暗号化し、この暗号化した第１の鍵を前記端末装置に対し送信する第４のステップと、

前記端末装置において、前記第１のＩＣカードから送信された暗号化された第１の鍵を受信し、この受信した暗号化された第１の鍵を付加した暗号鍵設定命令を前記第２のＩＣカードに対し送信する第５のステップと、

前記第２のＩＣカードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された暗号化された第１の鍵を前記第２のステップで記憶された第２の鍵により復号化し、この復号化した第１の鍵を記憶する第６のステップと、

を具備したことを特徴とするＩＣカード複製方法。

【請求項１２】　前記第１のＩＣカードに記憶されているデータを暗号化あるいは復号化するための第１の鍵は、前記端末装置から入力された鍵生成命令に基づき該第１のＩＣカード内で生成されたものであることを特徴とする請求項１１記載のＩＣカード複製方法。

【請求項１３】　前記第１のＩＣカードに記憶されているデータを暗号化あるいは復号化するための第１の鍵は、外部で生成され、前記端末装置を介して入力されたものであることを特徴とする請求項１１記載のＩＣカード複製方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、たとえば、内部で生成したデータを暗号化あるいは復号化するための鍵を別の鍵で暗号化して外部へ取出すことのできるＩＣカードに関する。

【０００２】

また、本発明は、上記ＩＣカードを用いてその複製カード（たとえば、バックアップカード）を作成するＩＣカード端末装置およびＩＣカード複製方法に関する。

【０００３】

【従来の技術】

最近、携帯可能な記憶媒体として、不揮発性のデータメモリとそれを制御する

ためのＣＰＵ（セントラル・プロセッシング・ユニット）を有するＩＣチップを内蔵した、いわゆるＩＣカードが産業各方面で利用されてきている。

【０００４】

この種のＩＣカードは、通常、カード発行会社などに設置されているＩＣカード発行装置を用いて発行される。このＩＣカード発行装置では、ＩＣカードを機能させるのに必要な命令データ、磁気エンコードデータ、印刷データなどをホストコンピュータにより作成し、それを発行機に順次伝送し、命令データについては、ＩＣカード内のＩＣチップへ入力し、磁気エンコードデータおよび印刷データについては、ＩＣカードの表面に磁気記録および印刷するようにしている。

【０００５】

ＩＣカード内のＩＣチップに対する命令データに伴い実行される処理は、ＩＣカード発行処理の上で最も重要な処理の１つである。ＩＣカード内のＩＣチップは、伝送された個々の命令データの処理が正常に行なえたか否かの情報を出力する手段を備えていて、発行装置はＩＣチップからの出力情報を基に命令データを正常に伝送できたか否かを判断する手段を備えている。

【０００６】

また、ＩＣカードは、高いセキュリティを確保するために複数の鍵をデータメモリに設定記憶し、この複数の鍵を利用してデータの隠蔽やデータの正当性の確認処理などを行なうようになっている。

【０００７】

さらに、最近、たとえば、ネットワークにつながれた複数のパーソナルコンピュータのセキュリティを高めるために、ＩＣカードを利用する方法が開発されており、ＩＣカード内に記憶された鍵を利用して、電子データファイルの隠蔽やデータの正当性の確認処理などを行なう方法が利用されている。

【０００８】

また、より高いセキュリティを確保するために、複数の鍵をＩＣカード内のＣＰＵで生成することにより、鍵設定時の外部への漏洩を防止する方法がとられている。

【０００９】

【発明が解決しようとする課題】

ところが、上述した複数の鍵をＩＣカード内で生成する従来のＩＣカードシステムにおいて、ＩＣカードが破壊されたり、ＩＣカードを紛失したりすると、ＩＣカード内で生成した複数の鍵を利用して隠蔽や正当性の確認などを行なった電子データファイルを使用できなくなるという問題があった。

【００１０】

また、ＩＣカード内で生成した複数の鍵を容易にＩＣカード外に取出すことができると、セキュリティが著しく低下するという問題があった。

【００１１】

そこで、最近、たとえば、特開２０００－２６８１３７号公報に開示されているようなＩＣカードのバックアップ方法が考えられている。このＩＣカードのバックアップ方法は、正規のＩＣカードを識別するための識別情報を含むカード情報を、正規のＩＣカードから予備のＩＣカード内に複写しておき、必要に応じて、この予備のＩＣカードを正規のＩＣカードとする内容に上記識別情報を変更して、予備のＩＣカードを正規のＩＣカードに変更することにより、ＩＣカードの再発行を行なう技術である。

【００１２】

しかし、このＩＣカードのバックアップ方法は、全く同じＩＣカードを複製するものではない。したがって、再発行されたＩＣカードを用いても、前述したような問題を解決することはできない。

【００１３】

本発明は、上記課題を解決するためになされたもので、内部に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出すことのできるＩＣカードを提供することを目的とする。

【００１４】

また、本発明は、ＩＣカード内に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出し、それを別のＩＣカード内に記憶することにより、その複製カード（たとえば、バックアップカード）を容易に作成することのできるＩＣカード端末装置およびＩＣカード複製方法を提供することを目的と

する。

【００１５】

【課題を解決するための手段】

本発明のＩＣカードは、外部装置との間でデータを通信する通信手段と、データを暗号化あるいは復号化するための第１の鍵を記憶している記憶手段と、前記通信手段を介して受信されたデータが鍵設定命令である場合、この鍵設定命令に付加された第２の鍵を前記記憶手段に記憶せしめる鍵設定手段と、前記通信手段を介して受信されたデータが鍵取出命令である場合、前記鍵設定手段により前記記憶手段に記憶された第２の鍵で前記記憶手段内の第１の鍵を暗号化し、この暗号化した第１の鍵を前記通信手段を介して外部へ出力する鍵出力手段とを具備している。

【００１６】

また、本発明のＩＣカード端末装置は、一方には少なくともデータを暗号化あるいは復号化するための鍵が記憶され、他方には該鍵が記憶されていない２つのＩＣカードとの間でデータを通信する通信手段と、前記鍵が記憶された一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内の鍵を前記通信手段を介して取出す鍵取出手段と、前記鍵が記憶されていない他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該鍵を前記他方のＩＣカード内に記憶せしめる暗号鍵設定手段とを具備している。

【００１７】

また、本発明のＩＣカード端末装置は、２つのＩＣカードとの間でデータを通信する通信手段と、前記２つのＩＣカードに対し、第１の鍵を暗号化あるいは復号化するための第２の鍵を付加した鍵設定命令を前記通信手段を介して送信することにより、該第２の鍵を前記２つのＩＣカード内にそれぞれ記憶せしめる第１の鍵設定手段と、この第１の鍵設定手段による前記第２の鍵の設定が正常に終了したことを確認する確認手段と、この確認手段により第２の鍵の設定が正常に終了したことが確認されると、前記２つのＩＣカードのうち一方のＩＣカードに対

し鍵生成命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内においてデータを暗号化あるいは復号化するための前記第１の鍵を生成せしめる鍵生成手段と、この鍵生成手段により第１の鍵を生成させた前記一方のＩＣカードに対し鍵取出命令を前記通信手段を介して送信することにより、前記一方のＩＣカード内で生成された第１の鍵を前記通信手段を介して取出す鍵取出手段と、前記２つのＩＣカードのうち他方のＩＣカードに対し前記鍵取出手段により前記一方のＩＣカードから取出した第１の鍵を付加した暗号鍵設定命令を前記通信手段を介して送信することにより、該第１の鍵を前記他方のＩＣカード内に記憶せしめる第２の鍵設定手段とを具備している。

【００１８】

また、本発明のＩＣカード複製方法は、少なくともデータを暗号化あるいは復号化するための鍵が記憶されている被複製用の第１のＩＣカードと、複製用の第２のＩＣカードと、これら第１、第２のＩＣカードを取扱う端末装置とを有し、前記端末装置から前記第１のＩＣカードに対し鍵取出命令を送信する第１のステップと、前記第１のＩＣカードにおいて、前記端末装置から送信された鍵取出命令を受信し、前記鍵を前記端末装置に対し送信する第２のステップと、前記端末装置において、前記第１のＩＣカードから送信された鍵を受信し、この受信した鍵を付加した暗号鍵設定命令を前記第２のＩＣカードに対し送信する第３のステップと、前記第２のＩＣカードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された鍵を記憶する第４のステップとを具備している。

【００１９】

また、本発明のＩＣカード複製方法は、少なくともデータを暗号化あるいは復号化するための第１の鍵が記憶されている被複製用の第１のＩＣカードと、複製用の第２のＩＣカードと、これら第１、第２のＩＣカードを取扱う端末装置とを有し、前記端末装置から前記第１、第２のＩＣカードに対し、前記第１の鍵を暗号化あるいは復号化するための第２の鍵を付加した鍵設定命令を送信する第１のステップと、前記第１、第２のＩＣカードにおいて、前記端末装置から送信された鍵設定命令を受信し、その鍵設定命令に付加された第２の鍵をそれぞれ記憶す

る第２のステップと、前記端末装置から前記第１のＩＣカードに対し鍵取出命令を送信する第３のステップと、前記第１のＩＣカードにおいて、前記端末装置から送信された鍵取出命令を受信し、前記第２のステップで記憶された第２の鍵により前記第１の鍵を暗号化し、この暗号化した第１の鍵を前記端末装置に対し送信する第４のステップと、前記端末装置において、前記第１のＩＣカードから送信された暗号化された第１の鍵を受信し、この受信した暗号化された第１の鍵を付加した暗号鍵設定命令を前記第２のＩＣカードに対し送信する第５のステップと、前記第２のＩＣカードにおいて、前記端末装置から送信された暗号鍵設定命令を受信し、その暗号鍵設定命令に付加された暗号化された第１の鍵を前記第２のステップで記憶された第２の鍵により復号化し、この復号化した第１の鍵を記憶する第６のステップとを具備している。

【００２０】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して説明する。

【００２１】

図１は、本発明の実施の形態に係るＩＣカード発行システムの構成例を概略的に示すものである。図１において、このＩＣカード発行システムは、端末装置２００およびカード発行装置２１０を備えていて、両者はケーブル２０５を介して接続されている。端末装置２００は、たとえば、パーソナルコンピュータ（ＰＣ）であり、端末本体２０１、補助記憶装置としてのハードディスク装置（ＨＤＤ）２０２、入力装置としてのキーボード２０３、および、ディスプレイ２０４を備えている。

【００２２】

端末本体２０１は、演算部としてのＣＰＵ（セントラル・プロセッシング・ユニット）２０１ａ、および、主記憶装置としてのメモリ２０１ｂを備えている。ＣＰＵ２０１ａは、本発明のポイントである鍵設定処理を制御する。また、端末本体２０１は、ハードディスク装置２０２、キーボード２０３、および、ディスプレイ２０４とそれぞれ接続されている。

【００２３】

ハードディスク装置２０２には、データ項目定義ファイルＦ１１、磁気エンコード用データベースファイルＦ１２、個人データベースファイルＦ１３、共通データベースファイルＦ１４、命令コードデータベースファイルＦ１５、および、印刷デザイン定義ファイルＦ１６などが格納されている。

【００２４】

カード発行装置２１０は、カードリーダ・ライタ２０６、カード印刷機２０７、磁気エンコーダ２０８、カード供給部２１１、スタッカ２１２を備えていて、カード供給部２１１にセットされた発行すべきＩＣカード１００を１枚ずつ取込み、取込んだＩＣカード１００を該カード発行装置２１０内を経由させた後、カードスタッカ２１２へ排出するようになっている。

【００２５】

ＩＣカード１００は、たとえば、図２に示すように、コンタクト部１０５、ＩＣチップ１０６、および、磁気ストライプ部１０７を備えている。ＩＣチップ１０６は、制御素子１０１、データメモリ１０２、ワーキングメモリ１０３、および、プログラムメモリ１０４を備えている。コンタクト部１０５およびＩＣチップ１０６は一体的にモジュール化され、ＩＣカード本体に埋設されている。

【００２６】

制御素子１０１は、たとえば、ＣＰＵである。この制御素子１０１は、本発明のポイントである鍵設定処理、鍵生成処理、鍵暗号化処理などを実行する。データメモリ１０２は、記憶内容が消去可能な不揮発性のメモリであり、たとえば、ＥＥＰＲＯＭ（electrically erasable and programmable ROM）である。ワーキングメモリ１０３は、制御素子１０１の処理データなどを一時的に格納するメモリであり、たとえば、ＲＡＭ（random access memory）である。プログラムメモリ１０４は、制御素子１０１のプログラムなどを記憶するメモリであり、たとえば、マスクＲＯＭ（read only memory）である。コンタクト部１０５は、カード発行装置２１０のカードリーダ・ライタ２０６と電気的に接触する部分であり、このコンタクト部１０５およびカードリーダ・ライタ２０６を介してカード発行装置２１０とＩＣカード１００との間で各種データ交換が行なわれる。

【００２７】

カード発行装置２１０のカードリーダ・ライタ２０６は、ＩＣカード１００のコンタクト部１０５を介してＩＣカード１００との間で各種データ交換を行なう。また、カードリーダ・ライタ２０６は、ＩＣカード１００の磁気ストライプ部１０７に対して各種データを磁気記録したり、磁気ストライプ部１０７に磁気記録された各種データを読出したりもする。

【００２８】

カード発行装置２１０は、以下に示す［１］～［４］の各機能をそれぞれ備えている。

【００２９】

［１］端末装置２００からカード発行装置２１０に送られた命令データをＩＣカード１００のコンタクト部１０５を介して制御素子１０１に送信する機能（カードリーダ・ライタ２０６）。

【００３０】

［２］ＩＣカード１００の制御素子１０１から送られた応答をコンタクト部１０５を介してカード発行装置２１０から端末装置２００に送信する機能（カードリーダ・ライタ２０６）。

【００３１】

［３］端末装置２００からカード発行装置２１０に送られた印刷データをＩＣカード１００の表面に印刷する機能（カード印刷機２０７）。

【００３２】

［４］端末装置２００からカード発行装置２１０に送られた磁気エンコードデータをＩＣカード１００の磁気ストライプ部１０７に磁気記録する機能（磁気エンコーダ２０８）。

【００３３】

図３は、カード発行装置２１０、端末装置２００側から送信された命令（鍵設定命令、鍵生成命令、鍵取出命令など）に対してＩＣカード１００側から出力される出力情報（レスポンス）のフォーマット例を示すものである。なお、鍵設定命令、鍵生成命令、鍵取出命令の各機能については後に説明する。

【００３４】

図３（ａ）に示す第１のフォーマットは、ステータスコードを出力情報として含む。このステータスコードは、カード発行装置２１０側から送信された命令の実行結果を示す。

【００３５】

図３（ｂ）に示す第２のフォーマットは、データ部およびステータスコードを出力情報として含む。このステータスコードは、上記同様にカード発行装置２１０側から送信された命令の実行結果を示す。なお、データ部については後で詳細に説明する。

【００３６】

図４は、ＩＣカード１００のデータメモリ１０２におけるファイル構造の一例を示すものである。

【００３７】

図４（ａ）は、Ａさんが所持するＩＣカード１００ａ（ＩＣカードａと表記することもある）のデータメモリ１０２におけるファイル構造を示しており、メインファイル（ＭＦ）を中心として、このメインファイル（ＭＦ）に複数のサブファイル（ＩＥＦ１、ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５、ＩＥＦ６、ＷＥＦ１、ＷＥＦ２）がぶら下がる構造になっている。サブファイル（ＩＥＦ１、ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５、ＩＥＦ６）は、鍵格納部として機能し、サブファイル（ＩＥＦ１）には鍵１（Ａ）が格納され、サブファイル（ＩＥＦ２）には鍵２（Ａ）が格納され、サブファイル（ＩＥＦ３）には鍵３（Ａ）が格納され、サブファイル（ＩＥＦ４）には復号化用鍵Ａが格納され、サブファイル（ＩＥＦ５）には暗号化用鍵Ａが格納され、サブファイル（ＩＥＦ６）には暗号化用鍵Ｂが格納される。これら、鍵１（Ａ）、鍵２（Ａ）、鍵３（Ａ）を合わせて鍵群（第２の鍵）と称し、復号化用鍵（Ａ）、暗号化用鍵（Ａ）、暗号化用鍵（Ｂ）をシステムで利用する本鍵（第１の鍵）とする。また、サブファイル（ＷＥＦ１）にはＡさんの会員番号（Ａ）が格納され、サブファイル（ＷＥＦ２）には該カードの有効期限（Ａ）が格納される。

【００３８】

図４（ｂ）は、Ａさんとは異なるＢさんが所持するＩＣカード１００ｂ（ＩＣ

カードｂと表記することもある）のデータメモリ１０２におけるファイル構造を示しており、上記同様、メインファイル（ＭＦ）を中心として、このメインファイル（ＭＦ）に複数のサブファイル（ＩＥＦ１、ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５、ＩＥＦ６、ＷＥＦ１、ＷＥＦ２）がぶら下がる構造になっている。サブファイル（ＩＥＦ１）には鍵１（Ｂ）が格納され、サブファイル（ＩＥＦ２）には鍵２（Ｂ）が格納され、サブファイル（ＩＥＦ３）には鍵３（Ｂ）が格納され、サブファイル（ＩＥＦ４）には復号化用鍵（Ｂ）が格納され、サブファイル（ＩＥＦ５）には暗号化用鍵（Ｂ）が格納され、サブファイル（ＩＥＦ６）には暗号化用鍵（Ａ）が格納される。これら、鍵１（Ｂ）、鍵２（Ｂ）、鍵３（Ｂ）を合わせて鍵群（第２の鍵）と称し、復号化用鍵（Ｂ）、暗号化用鍵（Ｂ）、暗号化用鍵（Ａ）をシステムで利用する本鍵（第１の鍵）とする。また、サブファイル（ＷＥＦ１）にはＢさんの会員番号（Ｂ）が格納され、サブファイル（ＷＥＦ２）には該カードの有効期限（Ｂ）が格納される。

【００３９】

ＩＣカード１００のＩＣチップ１０６内では、本鍵を利用してデータの隠蔽とデータの正当性の確認処理が行なわれる。ＩＣチップ１０６内では、鍵群を利用して本鍵の暗号化が行なわれる。本鍵は、セキュリティを高めるため、ＩＣチップ１０６内で生成されるものである。鍵群は、本鍵を暗号化するもので、カード発行時にカード発行装置２１０で生成される鍵設定命令、後述する個人端末装置で生成される鍵設定命令、あるいは、特殊鍵設定命令により設定されるものであり、正しい暗号化を実行させるためには正しい鍵群が設定されなければならない。

【００４０】

図５は、ＩＣカード１００内の鍵を利用するシステム例を示すものである。

【００４１】

図５において、ＩＣカード端末装置としての個人端末装置３００（個人端末装置（Ａ）と表記することもある）はＡさんが所持し、同じく個人端末装置４００（個人端末装置（Ｂ）と表記することもある）はＢさんが所持し、これら個人端末装置３００と個人端末装置４００とはネットワークやＬＡＮなどの通信回線５

００を介して接続されていて、両者の間で各種データの交換や各種電子データファイルの交換が行なわれるようになっている。

【００４２】

個人端末装置３００は、たとえば、パーソナルコンピュータ（ＰＣ）であり、端末本体３０１、補助記憶装置としてのハードディスク装置（ＨＤＤ）３０２、入力装置としてのキーボード３０３、および、ディスプレイ３０４を備えている。

【００４３】

端末本体３０１は、演算部としてのＣＰＵ３０１ａ、および、主記憶装置としてのメモリ３０１ｂを備えている。ＣＰＵ３０１ａは、本発明のポイントである鍵設定処理を制御する。また、端末本体３０１は、ハードディスク装置３０２、キーボード３０３、および、ディスプレイ３０４、および、カードリーダ・ライタ３０６（カードリーダ・ライタＡと表記することもある）とそれぞれ接続されている。ハードディスク装置３０２には、暗号化用鍵Ａで暗号化された機密情報である電子データファイルＦ２１、Ｆ２２、Ｆ２３などが格納されている。なお、電子データファイルは、たとえば、電子メール、文書ファイル、プログラムソースなどである。

【００４４】

個人端末装置３００は、カードリーダ・ライタ３０６を介してＩＣカード１００ａとの間で各種データの交換を行なう。

【００４５】

個人端末装置４００も上記同様に構成されている。すなわち、個人端末装置４００は、たとえば、パーソナルコンピュータ（ＰＣ）であり、端末本体４０１、補助記憶装置としてのハードディスク装置（ＨＤＤ）４０２、入力装置としてのキーボード４０３、および、ディスプレイ４０４を備えている。

【００４６】

端末本体４０１は、演算部としてのＣＰＵ４０１ａ、および、主記憶装置としてのメモリ４０１ｂを備えている。ＣＰＵ４０１ａは、本発明のポイントである鍵設定処理を制御する。また、端末本体４０１は、ハードディスク装置４０２、

キーボード４０３、および、ディスプレイ４０４、および、カードリーダ・ライタ４０６（カードリーダ・ライタＢと表記することもある）とそれぞれ接続されている。ハードディスク装置４０２には、暗号化用鍵Ｂで暗号化された機密情報である電子データファイルＦ３１、Ｆ３２、Ｆ３３などが格納されている。

【００４７】

個人端末装置４００は、カードリーダ・ライタ４０６を介してＩＣカード１００ｂとの間で各種データの交換を行なう。

【００４８】

個人端末装置３００と個人端末装置４００とは、上記したように、ネットワークやＬＡＮなどの通信回線５００を介して各種データの交換や各種電子データファイルの交換が行なわれる。その場合、セキュリティを高めるために、たとえば、個人端末装置４００から個人端末装置３００に電子データファイルを送る場合、個人端末装置４００は、まず、カードリーダ・ライタ４０６を介してＩＣカード１００ｂに対して、たとえば、電子データファイル１（電子データファイルＦ３１）を付加した暗号化用鍵（Ａ）での暗号化命令を送信する。

【００４９】

ＩＣカード１００ｂのコンタクト部１０５で受信された暗号化用鍵（Ａ）での暗号化命令は、制御素子１０１で解読される。この解読の際、暗号化用鍵（Ａ）での暗号化命令であることが判明し、この解読結果に基づき、暗号化命令に付加された電子データファイル１を復号化用鍵Ｂで復号化を行ない、その後、暗号化用鍵Ａを使用して暗号化を行ない、暗号化命令に対するレスポンスとして、正常終了情報および暗号化結果がコンタクト部１０５からカードリーダ・ライタ４０６を介して個人端末装置４００に送信される。

【００５０】

個人端末装置４００は、ＩＣカード１００ｂからのレスポンス情報（暗号化用鍵Ａで暗号化された電子データファイル１）を個人端末装置３００に送る。個人端末装置３００は、受取った情報（暗号化用鍵Ａで暗号化された電子データファイル１）をハードディスク装置３０２の電子データファイルＦ２１に保存する。受取った情報（暗号化用鍵Ａで暗号化された電子データファイル１）を閲覧する

場合、端末装置３００は、まず、カードリーダ・ライタ３０６を介してＩＣカード１００ａに対して、暗号化用鍵Ａで暗号化された電子データファイル１（電子データファイルＦ２１）を付加した復号化用鍵（Ａ）での復号化命令を送信する。

【００５１】

ＩＣカード１００ａのコンタクト部１０５で受信された復号化用鍵（Ａ）での復号化命令は、制御素子１０１で解読される。この解読の際、復号化用鍵（Ａ）での復号化命令であることが判明し、この解読結果に基づき、復号化命令に付加された電子データファイル１を復号化鍵用Ａで復号化を行ない、復号化命令に対するレスポンスとして、正常終了情報および復号化結果がコンタクト部１０５からカードリーダ・ライタ３０６を介して個人端末装置３００に送信される。

【００５２】

このように、ＩＣカード内の復号化用鍵を利用して、ＩＣカード内でのみ復号化を行なうためセキュリティが高いが、たとえば、ＩＣカードの破損などで復号化用鍵を失った場合は、個人端末装置３００のハードディスク装置３０２に保存されている電子データファイルを復号化することが不可能となる。また、個人端末装置４００から送られてくるデータを復号化することも不可能となる。

【００５３】

そこで、本発明では、以下に詳細を説明するバックアップカード（バックアップ用のＩＣカードと表記することもある）の作成処理にしたがい、カード発行装置２１０によりＩＣカード１００に対して、本カード（正規のＩＣカード）の作成およびバックアップカード（正規のＩＣカードの複製カード）の作成を行ない、個人端末装置３００または４００において、本カード内で暗号化用鍵および復号化用鍵の生成を行ない、即時にバックアップカードを作成することで、本カードの破損時にバックアップカードを使うことにより、電子データファイルの復号化を行ない、新しいＩＣカードで暗号化を行なうことにより、電子データファイルが復号化不可能となることを防止するものである。

【００５４】

まず、図６ないしい図１０を参照してＩＣカード発行システムの端末装置２０

０で生成される命令データの生成方法について説明する。

【００５５】

端末装置２００のハードディスク装置２０２内に保管されている個人データベースファイルＦ１３は、たとえば、図６に示すように、漢字氏名（項目１）、漢字住所（項目２）、カナ名字（項目３）、会員番号（項目４）、有効期限（項目５）、パスワード（項目６）、鍵１（項目７）などの個別データを１レコードとしたレコード群（個別データ群）から構成されている。

【００５６】

また、ハードディスク装置２０２内に保管されている本カード用の命令コードデータベースファイルＦ１５は、ＩＣカード１００のＩＣチップ１０６内の制御素子１０１に対して条件設定を行なったり、付加データをデータメモリ１０２に書込ませる働きをする命令コードなどから構成される。たとえば、図７に示すように、命令コード欄、付加データ欄、ＩＣ出力情報欄が用意されており、図７の例では、たとえば、「命令コード１８」の付加データは「個人データベースファイルの項目６」が定義されて、ＩＣ出力情報は「９０００」と比較すると定義され、「命令コード２５」の付加データは「個人データベースファイルの項目５」が定義されて、ＩＣ出力情報は「９０００」と比較すると定義されている。

【００５７】

端末装置２００は、命令コードデータベースと個人データベースとから、たとえば、図１０に示すように、命令コード１９に付加データとして個人データベースファイルの項目７のデータ「49 83..6c 44 78 」が付加された命令データを生成する。

【００５８】

たとえば、復号化用鍵取出し・設定命令用鍵群の鍵１は次のように設定する。端末装置２００は、ハードディスク装置２０２内に格納されている命令コードデータベースファイル（図７参照）の命令コード１９と、個人データベースファイル（図６参照）の項目７とから命令データを生成し、カードリーダ・ライタ２０６を介してＩＣカード１００のＩＣチップ１０６に送ることにより、鍵１を設定する。この命令コード１９を鍵設定命令と称する。

【００５９】

ＩＣカード１００のＩＣチップ１０６内での動作をさらに詳細に説明すると、カードリーダ・ライタ２０６からＩＣカード１００のコンタクト部１０５に対して、鍵１が付加された鍵設定命令が送信される。コンタクト部１０５で受信された鍵設定命令は、制御素子１０１で解読される。この解読の際、鍵１の設定命令であることが判明し、この解読結果に基づき鍵１がデータメモリ１０２のサブファイル（ＩＥＦ１）に設定（記憶）される。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・ライタ２０６に送信される。すなわち、正常終了情報が端末本体２０１に通知されることになる。

【００６０】

バックアップカード用の命令コードデータベースファイルは、本カード用命令コードデータベースファイルと同様に、ＩＣカード１００のＩＣチップ１０６内の制御素子１０１に対して条件設定を行なったり、付加データをデータメモリ１０２に書込ませる働きをする命令コードなどから構成される。たとえば、図８に示すように、命令コード欄、付加データ欄、ＩＣ出力情報欄が用意されており、図８の例では、たとえば、「命令コード１８」の付加データは「個人データベースファイルの項目６」が定義されている。

【００６１】

バックアップカードは、たとえば、図９に示すように、本カードとしての機能を果たすための必須情報である会員番号や有効期限の情報がないファイル構造となっている。したがって、バックアップカード用の命令コードデータベースファイルは、本カード用の命令コードデータベースファイルと異なり、鍵１の設定情報以降の命令コードは定義されない。

【００６２】

次に、本カードおよびバックアップカードの発行処理について、図１１に示すフローチャートを参照して説明する。

【００６３】

まず、カード供給部２１１からＩＣカード１００を取込み（Ｓ１０１）、その

後、本カード用の命令コードデータベースファイルＦ１５に基づき命令コードを生成して（Ｓ１０２）、それをＩＣカード１００に送る（Ｓ１０３）。

【００６４】

次に、本カード用の印刷デザイン定義ファイルＦ１６に基づきカード表面の印刷データを生成し、この生成した印刷データをカード印刷機２０７へ送ることにより、ＩＣカード１００の表面に印刷を行なう（Ｓ１０４）。

【００６５】

次に、本カード用の磁気エンコード用データベースファイルＦ１２に基づき磁気記録データを生成し、この生成した磁気記録データを磁気エンコーダ２０８へ送ることにより、ＩＣカード１００磁気ストライプ部１０７に磁気記録を行なう（Ｓ１０５）。

【００６６】

次に、本カードの発行処理が正常に終了したかを確認し（Ｓ１０６）、正常に終了した場合、該ＩＣカード１００をスタッカ２１２に排出する（Ｓ１０７）。スタッカ２１２に排出されたＩＣカード１００は本カードとして発行されたＩＣカードである。

【００６７】

スタッカ２１２に本カードを排出した後、カード供給部２１１から２枚目のＩＣカード１００を取込み、その後、バックアップカード用の命令コードデータベースファイルＦ１５に基づき命令コードを生成して（Ｓ１０８）、それをＩＣカード１００に送る（Ｓ１０９）。

【００６８】

次に、バックアップカード用の印刷デザイン定義ファイルＦ１６に基づきカード表面の印刷データを生成し、この生成した印刷データをカード印刷機２０７へ送ることにより、ＩＣカード１００の表面に印刷を行なう（Ｓ１１０）。

【００６９】

次に、バックアップカード用の磁気エンコード用データベースファイルＦ１２に基づき磁気記録データを生成し、この生成した磁気記録データを磁気エンコーダ２０８へ送ることにより、ＩＣカード１００の磁気ストライプ部１０７に磁気

記録を行なう（Ｓ１１１）。

【００７０】

次に、バックアップカードの発行処理が正常に終了したかを確認し（Ｓ１１２）、正常に終了した場合、該ＩＣカード１００をスタッカ２１２に排出する（Ｓ１１３）。スタッカ２１２に排出されたＩＣカード１００はバックアップカードとして発行されたＩＣカードである。

【００７１】

なお、ステップＳ１０６、Ｓ１１２において、カードの発行処理が正常に終了しなかった場合、該ＩＣカード１００を図示しないリジェクト部に排出する（Ｓ１１４）。

【００７２】

このようにして、本カードおよびバックアップカードの発行処理が行なわれるものであり、発行処理終了直後（カード製造者からの出荷状態）の両カードにおけるデータメモリ１０２の内部の状態を図１２に模式的に示す。上記した発行処理により、図に網掛けしたファイル（ＩＥＦ１、ＷＥＦ１、ＷＥＦ２）に所定のデータが設定（記憶）され、網掛けのない他のファイル（ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５、ＩＥＦ６）はデータ未設定の状態である。

【００７３】

次に、上記したように発行された本カードに暗号化用鍵および復号化用鍵を生成させ、バックアップカードに復号化用鍵を設定する処理について説明する。なお、以下の説明では個人端末装置３００を用いて行なう場合について述べるが、個人端末装置４００を用いても同様に行なえる。

【００７４】

まず、本カードに暗号化用鍵および復号化用鍵を生成させ、バックアップカードに復号化用鍵を設定するシステムの構成について図１３を参照して説明する。図１３において、個人端末装置３００には、本カード用のカードリーダ・ライタ３０６ａと共にバックアップカード用のカードリーダ・ライタ３０６ｂが接続されており、カードリーダ・ライタ３０６ａには前記のように発行された本カード１００ｃ（ＩＣカードａに対応、本カードａと表記することもある）が挿入され

、カードリーダ・ライタ３０６ｂには前記のように発行されたバックアップカード１００ｄ（バックアップカードａと表記することもある）が挿入される。

【００７５】

個人端末装置３００のディスプレイ３０４には、図１４に示すような鍵入力画面が表示される。この鍵入力画面には、復号化用鍵取出し・設定命令用鍵群のうち、前述の発行処理で設定を行なわなかった鍵を入力するエリア、および、鍵設定を行なうために必要な照合用パスワードの入力エリア、鍵入力の終了を指示する入力終了釦、処理を中断するための終了釦がそれぞれ表示されている。

【００７６】

設定対象となる鍵群（鍵２、鍵３）は、オペレータによるキーボード３０３の操作により端末本体３０１に入力される。全ての鍵（鍵２、鍵３）とパスワードの入力が終了し、入力終了釦により入力終了が指示されると、本カード１００ｃおよびバックアップカード１００ｄへの鍵の設定、本カード１００ｃでの暗号化用鍵、復号化用鍵の生成、本カード１００ｃから復号化用鍵の取出し、バックアップカード１００ｄへの復号化用鍵の設定が開始される。

【００７７】

次に、本カード１００ｃおよびバックアップカード１００ｄへの鍵の設定、本カード１００ｃでの暗号化用鍵および復号化用鍵の生成、本カード１００ｃからの復号化用鍵の取出し、バックアップカード１００ｄへの復号化用鍵の設定を行なう処理について、図１５に示すフローチャートを参照して説明する。

【００７８】

鍵の設定は、鍵設定命令により実行される。すなわち、カードリーダ・ライタ３０６ａを介して本カード１００ｃのコンタクト部１０５に対して、鍵２の鍵入力エリアに入力された鍵２が付加された鍵設定命令データが送信される（Ｓ２０１）。本カード１００ｃのコンタクト部１０５で受信された受信データは、制御素子１０１で解読される。この解読の際、受信データは鍵２の設定命令であることが判明すると、この解読結果に基づき鍵２がデータメモリ１０２のサブファイル（ＩＥＦ２）に設定（記憶）される（Ｓ２０１ａ）。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・

ライタ３０６ａに送信される。すなわち、正常終了情報が端末本体３０１に通知されることになる。

【００７９】

次に、カードリーダ・ライタ３０６ｂを介してバックアップカード１００ｄのコンタクト部１０５に対して、鍵２の鍵入力エリアに入力された鍵２が付加された鍵設定命令が送信され（Ｓ２０２）、上記同様に鍵２がバックアップカード１００ｄのデータメモリ１０２のサブファイル（ＩＥＦ２）に設定（記憶）される（Ｓ２０２ａ）。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ｂに送信される。すなわち、正常終了情報が端末本体３０１に通知されることになる。

【００８０】

この後、カードリーダ・ライタ３０６ａを介して本カード１００ｃのコンタクト部１０５に対して、鍵３の鍵入力エリアに入力された鍵３が付加された鍵設定命令が送信され（Ｓ２０３）、上記同様に鍵３が本カード１００ｃのデータメモリ１０２のサブファイル（ＩＥＦ３）に設定（記憶）される（Ｓ２０３ａ）。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ａに送信される。すなわち、正常終了情報が端末本体３０１に通知されることになる。

【００８１】

次に、カードリーダ・ライタ３０６ｂを介してバックアップカード１００ｄのコンタクト部１０５に対して、鍵３の鍵入力エリアに入力された鍵３が付加された鍵設定命令が送信され（Ｓ２０４）、上記同様に鍵３がバックアップカード１００ｄのデータメモリ１０２のサブファイル（ＩＥＦ３）に設定される（Ｓ２０４ａ）。そして、鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ｂに送信される。すなわち、正常終了情報が端末本体３０１に通知されることになる。

【００８２】

本カード１００ｃでの暗号化用鍵、復号化用鍵の生成は、暗号化用鍵・復号化用鍵生成命令により実行される。すなわち、カードリーダ・ライタ３０６ａを介

して本カード１００ｃのコンタクト部１０５に対して、暗号化用鍵・復号化用鍵生成命令データが送信される（Ｓ２０５）。コンタクト部１０５で受信された受信データは、制御素子１０１で解読される。この解読の際、受信データは暗号化用鍵・復号化用鍵生成命令であることが判明すると、この解読結果に基づき暗号化用鍵・復号化用鍵が生成され、データメモリ１０２のサブファイル（ＩＥＦ４、ＩＥＦ５）に設定（記憶）される（Ｓ２０５ａ）。そして、暗号化用鍵・復号化用鍵生成命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ａに送信される。すなわち、正常終了情報が端末本体３０１に通知されることになる。

【００８３】

本カード１００ｃから復号化用鍵の取出しは復号化用鍵取出命令により実行される。すなわち、カードリーダ・ライタ３０６ａを介して本カード１００ｃのコンタクト部１０５に対して、復号化用鍵取出命令データが送信される（Ｓ２０６）。コンタクト部１０５で受信された受信データは、制御素子１０１で解読される。この解読の際、受信データは復号化用鍵取出命令であることが判明すると、この解読結果に基づき、データメモリ１０２のサブファイル（ＩＥＦ４）に設定されている復号化用鍵を鍵群（鍵１、鍵２、鍵３）で暗号化した結果と正常終了情報が、復号化用鍵取出命令に対するレスポンスとして、コンタクト部１０５からカードリーダ・ライタ３０６ａに送信される（Ｓ２０６ａ、Ｓ２０７）。すなわち、正常終了情報と鍵群により暗号化された復号化用鍵が端末本体３０１に通知されることになる。

【００８４】

バックアップカード１００ｄへの復号化用鍵の設定は、上記で通知された鍵群により暗号化された復号化用鍵が付加された復号化用鍵設定命令により実行される。すなわち、カードリーダ・ライタ３０６ｂを介してバックアップカード１００ｄのコンタクト部１０５に対して、復号化用鍵設定命令データが送信される（Ｓ２０８）。コンタクト部１０５で受信された受信データは、制御素子１０１で解読される。この解読の際、受信データは復号化用鍵設定命令であることが判明すると、この解読結果に基づき、データメモリ１０２のサブファイル（ＩＥＦ１

、ＩＥＦ２、ＩＥＦ３）に設定されている鍵群（鍵１、鍵２、鍵３）で、復号化用鍵設定命令に付加された暗号化された復号化用鍵を復号化し、データメモリ１０２のサブファイル（ＩＥＦ４）に設定される（Ｓ２０８ａ）。そして、復号化用鍵設定命令に対するレスポンスとして、正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ｂに送信される。すなわち、正常終了情報が端末本体３０１に通知されることになる。

【００８５】

このようにして、本カード１００ｃに暗号化用鍵および復号化用鍵を生成させ、バックアップカード１００ｄに復号化用鍵を設定するものであり、処理終了直後（ユーザ使用開始前状態）の両カードにおけるデータメモリ１０２の内部の状態を図１６に模式的に示す。上記した処理により、図に縦破線、横破線、格子柄を付したファイル（ＩＥＦ２、ＩＥＦ３、ＩＥＦ４、ＩＥＦ５）に所定のデータが設定（記憶）され、何も付されてない他のファイル（ＩＥＦ６、ＩＥＦ５）はデータ未設定の状態である。

【００８６】

上記で説明した本カード１００ｃの作成およびバックアップカード１００ｄの作成の処理の模様を模式図で表わすと、図１７に示すようになる。

【００８７】

次に、このように作成された本カード１００ｃが破損し、個人端末装置３００の電子データファイルをバックアップカード１００ｄで復号化し、新しい本カードで暗号化する処理について説明する。なお、以下の説明では個人端末装置３００を用いて行なう場合について述べるが、個人端末装置４００を用いても同様に行なえる。

【００８８】

個人端末装置３００には、図１３を用いて先に説明したように、新しい本カード挿入用のカードリーダ・ライタ３０６ａと共にバックアップカード挿入用のカードリーダ・ライタ３０６ｂが接続されており、カードリーダ・ライタ３０６ａには新たに作成された本カード１００ｃが挿入され、カードリーダ・ライタ３０６ｂにはバックアップカード１００ｄが挿入される。

【００８９】

個人端末装置３００のディスプレイ３０４には、たとえば、図１８に示すようなファイル名入力画面が表示されている。このファイル名入力画面には、新しいカードで暗号化を行なうために必要な照合用パスワードの入力エリア、バックアップカードで復号化を行なうために必要な照合用パスワードの入力エリア、破損した旧い本カード１００ｃの暗号化用鍵で暗号化された電子データファイル名を入力する追加釦、電子データファイル名を表示するエリア、ファイル名入力の終了を指示する入力終了釦、処理を中断するための終了釦が表示されている。

【００９０】

オペレータによるキーボード３０３の操作により、破損した旧い本カード１００ｃの暗号化用鍵で暗号化された電子データファイル名の入力と、パスワードの入力が終了し、入力終了釦により入力終了が指示されると、バックアップカード１００ｄでの電子データファイルの復号化処理、および、新しい本カード１００ｃでの電子データファイルの暗号化処理が開始される。

【００９１】

以下、バックアップカード１００ｄでの電子データファイルの復号化処理、および、新しい本カード１００ｃでの電子データファイルの暗号化処理について、図１９に示すフローチャートを参照して説明する。

【００９２】

まず、入力されたバックアップカードで復号化を行なうために必要な照合用パスワードを基にバックアップカードで復号化を行なうために必要な照合の命令データが作成され、カードリーダ・ライタ３０６ｂを介してバックアップカード１００ｄに送信される（Ｓ３０１）。次に、新しいカードで暗号化を行なうために必要な照合用パスワードを基に新しいカードで暗号化を行なうために必要な照合の命令データが作成され、カードリーダ・ライタ３０６ａを介して新しい本カード１００ｃに送信される（Ｓ３０２）。

【００９３】

電子データファイルの復号化処理は、復号化命令により実行される。すなわち、カードリーダ・ライタ３０６ｂを介してバックアップカード１００ｄのコンタ

クト部１０５に対して、ファイル名入力エリアに入力された電子データファイルが付加された復号化命令が送信される（Ｓ３０３、Ｓ３０４）。

【００９４】

バックアップカード１００ｄのコンタクト部１０５で受信された復号化命令は、バックアップカード１００ｄの制御素子１０１で解読される。この解読の際、復号化命令であることが判明し、この解読結果に基づき、制御素子１０１は、データメモリ１０２のサブファイル（ＩＥＦ４）に設定されている復号化用鍵で復号化命令に付加されてきた電子データファイルを復号化し（Ｓ３０４ａ）、その復号化結果と正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ｂに送信する（Ｓ３０５）。

【００９５】

電子データファイルの暗号化処理は、暗号化命令により実行される。すなわち、カードリーダ・ライタ３０６ａを介して新しい本カード１００ｃのコンタクト部１０５に対して、上記で通知された復号化された電子データファイルが付加された暗号化命令が送信される（Ｓ３０６）。

【００９６】

新しい本カード１００ｃのコンタクト部１０５で受信された暗号化命令は、新しい本カード１００ｃの制御素子１０１で解読される。この解読の際、暗号化命令であることが判明し、この解読結果に基づき、制御素子１０１は、データメモリ１０２のサブファイル（ＩＥＦ５）に設定されている暗号化用鍵で暗号化命令に付加されてきた電子データファイルを暗号化し（Ｓ３０６ａ）、その暗号化結果と正常終了情報がコンタクト部１０５からカードリーダ・ライタ３０６ａを介して端末本体３０１に送信する（Ｓ３０７）。

【００９７】

端末本体３０１は、新しい本カード１００ｃからの暗号化用鍵で暗号化された電子データファイルをハードディスク装置３０２に格納する（Ｓ３０８）。次に、新しい本カード１００ｃから受取った暗号化された電子データファイルが最後の電子データファイルか否かを判断し（Ｓ３０９）、最後でなければステップＳ３０３からの動作を繰り返し、最後の電子データファイルになったところで処理

を終了する。

【００９８】

このように、上記実施の形態によれば、ＩＣカード内で生成された復号化用鍵、暗号化用鍵を外部へ取出す際、該ＩＣカード内に設定された別の複数の鍵で暗号化してから外部へ取出すことにより、安全に外部へ取出すことができる。そして、取出した復号化用鍵、暗号化用鍵を別のＩＣカードに書込むことにより、たとえば、バックアップカードを容易に作成できる。

【００９９】

したがって、たとえば、内部で生成した復号化用鍵、暗号化用鍵を持つＩＣカードが破壊しても、あらかじめ作成しておいたバックアップカードを用いることにより、該破壊したＩＣカード内の復号化用鍵、暗号化用鍵でデータの隠蔽や正当性の確認が行なわれた電子データファイルを再使用することが可能となる。

【０１００】

具体例を用いて更に詳細に説明する。たとえば、図５に示すシステムにおいて、個人端末装置３００と個人端末装置４００との間で電子メールの交換を行なっている場合で、たとえば、ＩＣカード１００ａが破損した場合、個人端末装置３００では、過去に個人端末装置４００から送られてきた電子メール、および、新たに個人端末装置４００から送られてきた電子メールを読むことが不可能となる。

【０１０１】

ところが、前述したようなバックアップカードを用いることにより、個人端末装置３００において、過去に個人端末装置４００から送られてきた電子メールを読むことができ、新しいＩＣカードを取得するまでの間、新たに個人端末装置４００から送られてきた電子メールを読むことや、個人端末装置４００に暗号化した電子メールを送ることが可能となる。

【０１０２】

なお、前記実施の形態では、鍵１をあらかじめ生成し、個人データベースファイルの一部としてハードディスク装置に格納しておくことで、ＩＣカードを発行する方法を説明したが、よりセキュリティを高めるため、たとえば、パーソナル

コンピュータのプログラム、または、専用の鍵生成装置などでカード発行時に自動的に鍵１を生成して、ＩＣカード内に設定する方法でもよい。このようにすれば、ハードディスク装置に格納しないため、セキュリティをより高くすることができる。

【０１０３】

また、同様に、鍵２、鍵３を画面入力する方法で説明したが、よりセキュリティを高めるため、たとえば、パーソナルコンピュータのプログラム、または、専用の鍵生成装置などでカード発行時に自動的に鍵２、鍵３を生成して、ＩＣカード内に設定する方法でもよい。

【０１０４】

また、復号化用鍵取出し・設定命令用鍵群の数が３つの場合について説明したが、たとえば、鍵１のみ、鍵１と鍵２のみ、あるいは、４つ以上の鍵としてもよい。

【０１０５】

また、本カード内にバックアップカード作成フラグを設けて、鍵群を使用して、復号化用鍵、暗号化用鍵が外部へ取出された場合には上記フラグを立て、フラグが立っている場合は鍵を外部へ取出すことができないようにすれば、さらにセキュリティを高めることができる。

【０１０６】

また、バックアップカードを作成した後は、本カードのデータメモリ内の鍵群エリアを鍵取出し不可とすることにより、鍵を取出すことができないようにしてもよい。

【０１０７】

また、復号化用鍵取出し・設定命令用鍵群の鍵１をカード発行時に、鍵２と鍵３をバックアップカードの作成時に、それぞれ設定する方法について説明したが、たとえば、図２０および図２１に示すように、鍵１、鍵２、鍵３を全てカード発行時に設定する方法でもよい。すなわち、カード製造者が鍵１、鍵２、鍵３を全て設定するものである。なお、図２０は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、図

２１は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、それぞれ示している。

【０１０８】

また、復号化用鍵取出し・設定命令用鍵群の鍵１をカード発行時に、鍵２と鍵３をバックアップカードの作成時に、それぞれ設定する方法について説明したが、たとえば、図２２および図２３に示すように、鍵１、鍵２、鍵３を全てバックアップカードの作成時に設定する方法でもよい。すなわち、ユーザが鍵１、鍵２、鍵３を全て設定するものである。なお、図２２は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、図２３は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、それぞれ示している。

【０１０９】

また、復号化用鍵、暗号化用鍵をバックアップカードの作成時に生成する方法について説明したが、たとえば、図２４および図２５に示すように、カード発行時に生成する方法でもよい。すなわち、鍵をカード製造者とユーザが分けて設定するものである。なお、図２４は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、図２５は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、それぞれ示している。

【０１１０】

また、復号化用鍵のみをバックアップカードに設定する方法について説明したが、新しいＩＣカードがユーザに届くまでの間に業務に支障が生じないように、たとえば、図２６および図２７に示すように、暗号化用鍵をもバックアップカードカードに設定する方法でもよい。なお、図２６は、カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、図２７は、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を、それぞれ示している。

【０１１１】

さらに、復号化用鍵、暗号化用鍵をＩＣカード内で生成する方法について説明

したが、たとえば、図２８に示すように、個人端末装置３００および個人端末装置４００を通信回線５００を介して認証局（鍵を生成するサービスセンタ）６００に接続し、認証局６００で生成された復号化用鍵、暗号化用鍵を例えば個人端末装置３００にダウンロードすることにより、本カード１００ｃに復号化用鍵、暗号化用鍵を設定するようにしてもよい。

【０１１２】

この場合の本カード１００ｃおよびバックアップカード１００ｄへの鍵の設定、本カード１００ｃへの暗号化用鍵および復号化用鍵の設定、本カード１００ｃからの復号化用鍵の取出し、バックアップカード１００ｄへの復号化用鍵の設定を行なう処理は、図２９に示すフローチャートのようになる。図２９のフローチャートは、前述した図１５のフローチャートに対し以下の点が若干異なる。すなわち、ステップＳ２０４とＳ２０５との間に認証局６００から本カード用の復号化用鍵、暗号化用鍵を取得するステップＳ２０９が追加される。また、ステップＳ２０５の処理が本カード用の復号化用鍵、暗号化用鍵設定命令の送信となるとともに、ステップＳ２０５ａの処理が復号化用鍵、暗号化用鍵の設定となる。

【０１１３】

この場合のカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を図３０に示し、ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリ１０２の内部の状態を図３１に示している。

【０１１４】

【発明の効果】

以上詳述したように本発明によれば、内部に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出すことのできるＩＣカードを提供できる。

【０１１５】

また、本発明によれば、ＩＣカード内に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出し、それを別のＩＣカード内に記憶することにより、その複製カード（たとえば、バックアップカード）を容易に作成す

ることのできるＩＣカード端末装置およびＩＣカード複製方法を提供できる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係るＩＣカード発行システムの構成例を概略的に示すブロック図。

【図２】

ＩＣカードの構成例を概略的に示すブロック図。

【図３】

ＩＣカード側から出力されるレスポンスのフォーマット例を示す図。

【図４】

ＩＣカードのデータメモリにおけるファイル構造の一例を示す図。

【図５】

ＩＣカードの鍵を利用するシステムの一例を示すブロック図。

【図６】

個人データベースファイルの一例を示す構成図。

【図７】

本カード用の命令コードデータベースファイルの一例を示す構成図。

【図８】

バックアップカード用の命令コードデータベースファイルの一例を示す構成図。

【図９】

バックアップカード用ＩＣカードのデータメモリにおけるファイル構造の一例を示す図。

【図１０】

命令データの一例を示す図。

【図１１】

本カードおよびバックアップカードの発行処理を説明するフローチャート。

【図１２】

カード製造者からの出荷状態の本カードおよびバックアップカードにおけるデ

ータメモリの内部状態を模式的に示す図。

【図１３】

発行された本カードに暗号化用鍵および復号化用鍵を生成させ、バックアップカードに復号化用鍵を設定するシステムの構成を示すブロック図。

【図１４】

鍵入力画面の一例を示す図。

【図１５】

本カードおよびバックアップカードへの鍵の設定、本カードでの暗号化用鍵および復号化用鍵の生成、本カードからの復号化用鍵の取出し、バックアップカードへの復号化用鍵の設定を行なう処理を説明するフローチャート。

【図１６】

ユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図１７】

本カードおよびバックアップカードの作成処理の模様を説明する模式図。

【図１８】

ファイル名入力画面の一例を示す図。

【図１９】

バックアップカードでの電子データファイルの復号化処理、および、新しい本カードでの電子データファイルの暗号化処理を説明するフローチャート。

【図２０】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２１】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２２】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２３】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２４】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２５】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２６】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２７】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図２８】

他の例において、発行された本カードに暗号化用鍵および復号化用鍵を設定し、バックアップカードに復号化用鍵を設定するシステムの構成を概略的に示すブロック図。

【図２９】

他の例において、本カードおよびバックアップカードへの鍵の設定、本カードへの暗号化用鍵および復号化用鍵の設定、本カードからの復号化用鍵の取出し、バックアップカードへの復号化用鍵の設定を行なう処理を説明するフローチャート。

【図３０】

他の例におけるカード製造者からの出荷状態の本カードおよびバックアップカードにおけるデータメモリの内部状態を模式的に示す図。

【図３１】

他の例におけるユーザ使用開始前状態の本カードおよびバックアップカードに

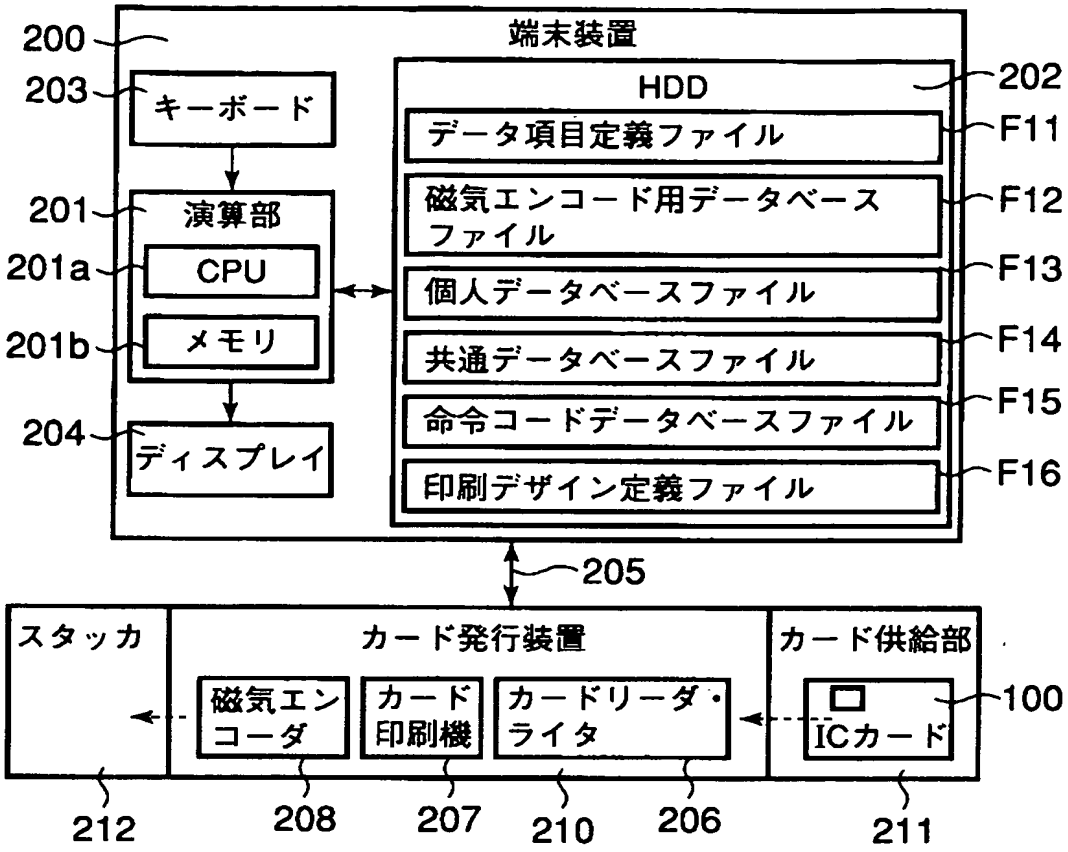
おけるデータメモリの内部状態を模式的に示す図。

【符号の説明】

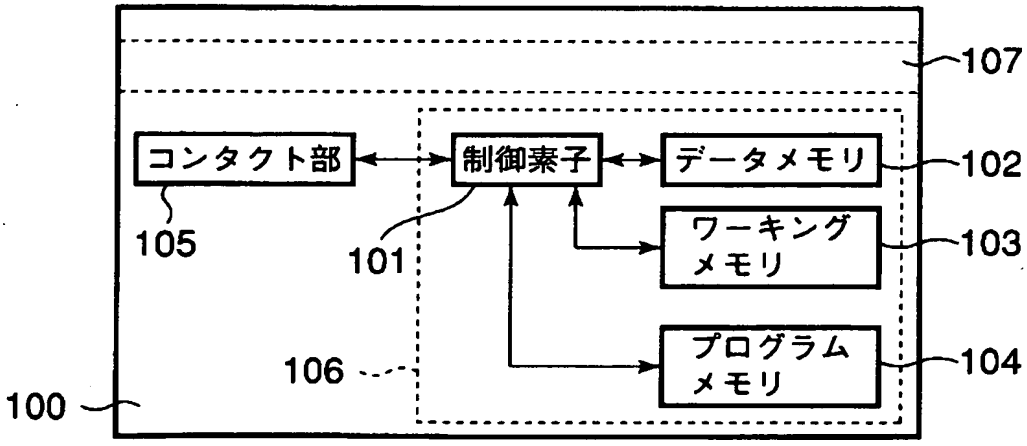
１００，１００ａ，１００ｂ…ＩＣカード、１００ｃ…本カード、１００ｄ…バックアップカード（複製カード）、１０１…制御素子、１０２…データメモリ、１０３…ワーキングメモリ、１０４…プログラムメモリ、１０５…コンタクト部、１０６…ＩＣチップ、２００…端末装置、２０１…端末本体、２０１ａ…ＣＰＵ、２０１ｂ…メモリ、２０２…ハードディスク装置、２０３…キーボード、２０４…ディスプレイ、２０６…カードリーダ・ライタ、２０７…カード印刷機、２０８…磁気エンコーダ、２１０…カード発行装置、２１１…カード供給部、２１２…カードスタッカ、３００…個人端末装置（ＩＣカード端末装置）、３０１…端末本体、３０１ａ…ＣＰＵ、３０１ｂ…メモリ、３０２…ハードディスク装置、３０３…キーボード、３０４…ディスプレイ、３０６ａ，３０６ｂ…カードリーダ・ライタ、４００…個人端末装置（ＩＣカード端末装置）、４０６…カードリーダ・ライタ、５００…通信回線。

【書類名】　　図面

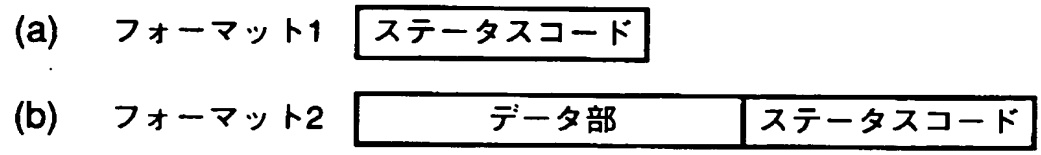
【図１】


200
端末装置
203
キーボード
201
演算部
201a
CPU
201b
メモリ
204
ディスプレイ
HDD
202
データ項目定義ファイル
F11
磁気エンコード用データベースファイル
F12
個人データベースファイル
F13
共通データベースファイル
F14
命令コードデータベースファイル
F15
印刷デザイン定義ファイル
F16
205
スタッカ
カード発行装置
カード供給部
磁気エンコーダ
カード印刷機
カードリーダ・ライタ
ICカード
100
212
208
207
210
206
211

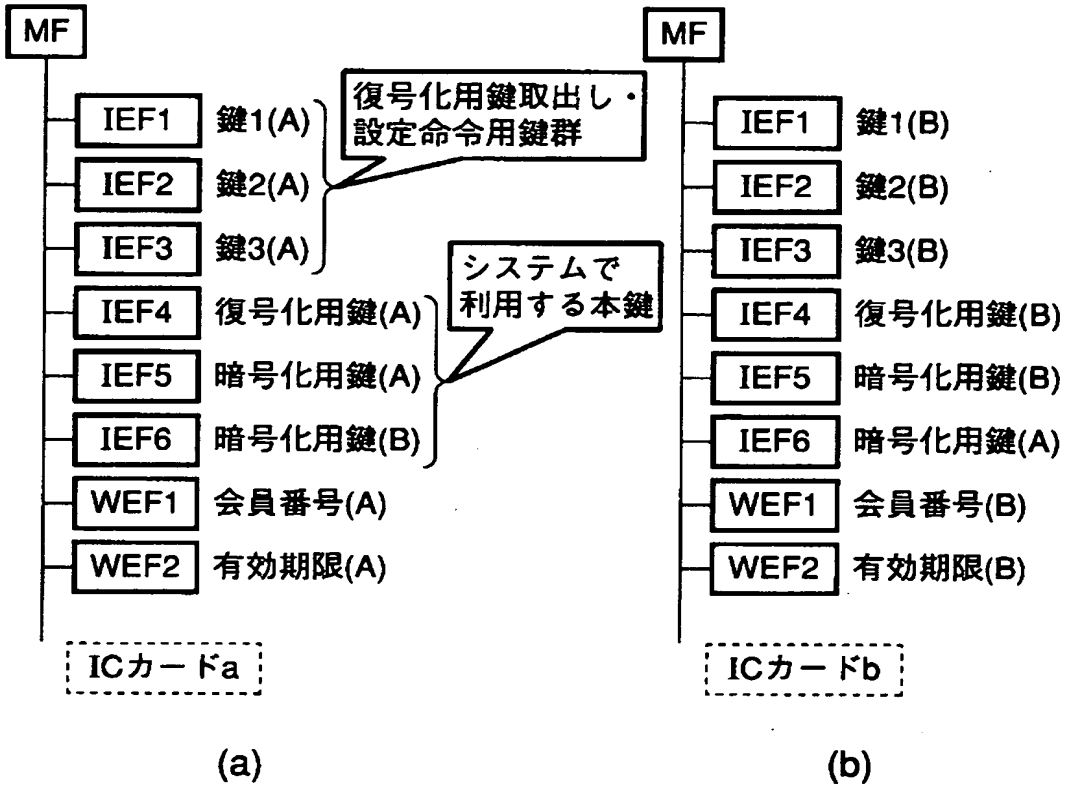
【図２】


107
コンタクト部
制御素子
データメモリ
102
105
101
ワーキングメモリ
103
106
プログラムメモリ
104
100

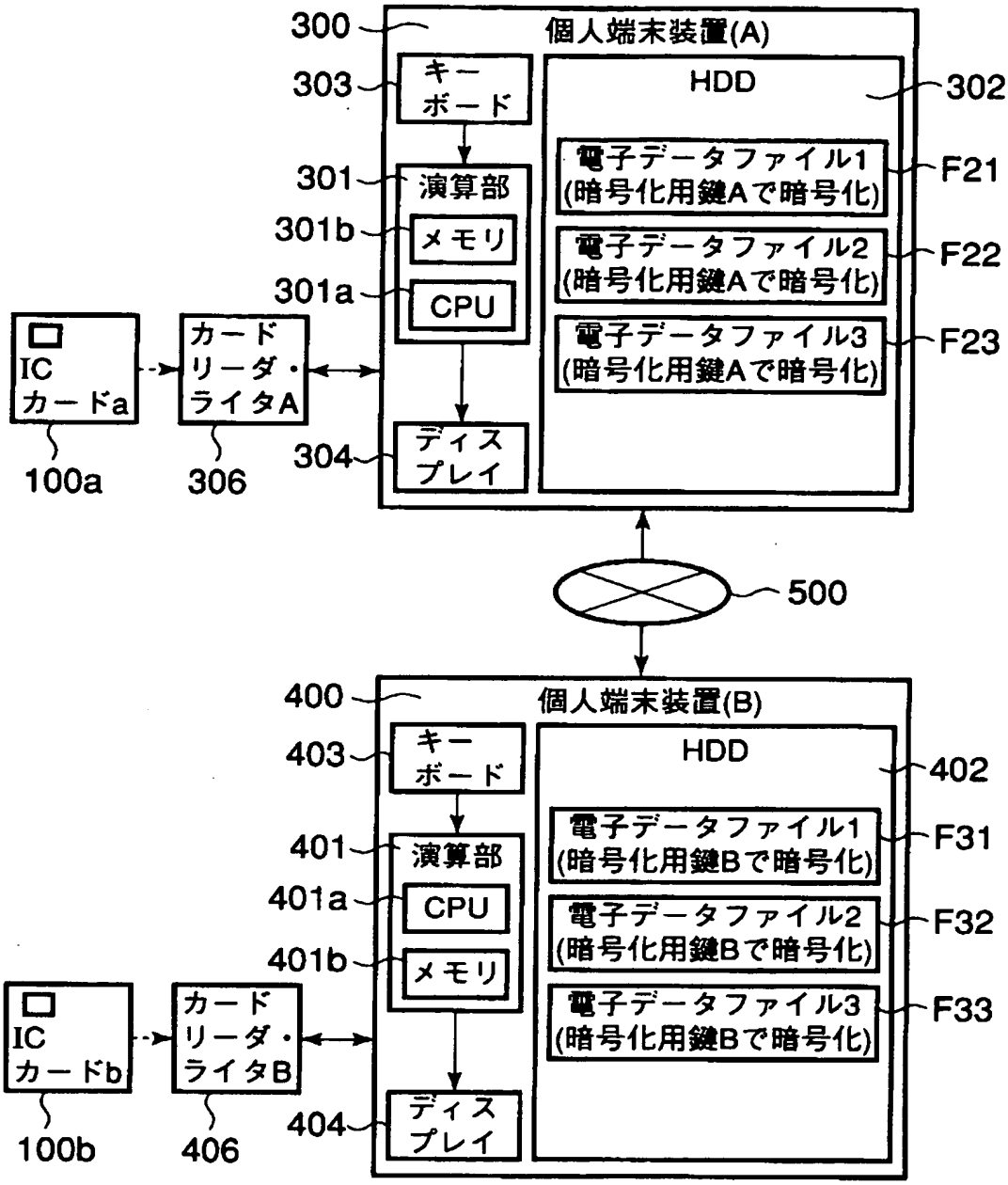
【図３】


(a)
フォーマット1
ステータスコード
(b)
フォーマット2
データ部
ステータスコード

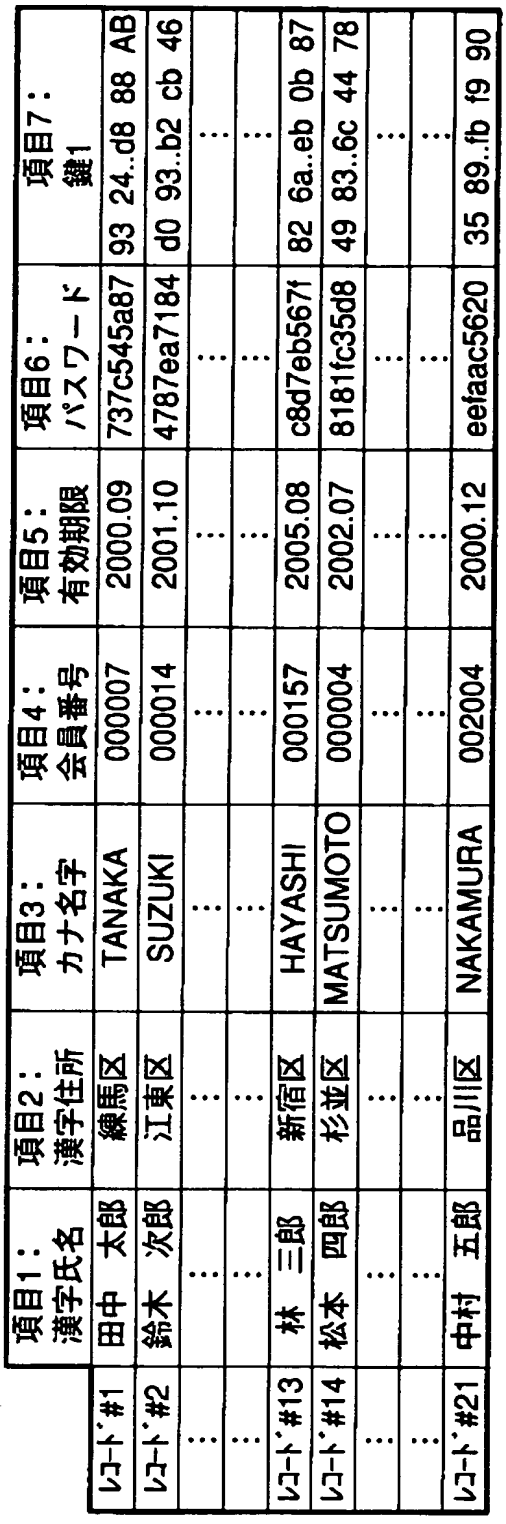
【図４】


MF
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
復号化用鍵取出し・設定命令用鍵群
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
システムで利用する本鍵
WEF1
会員番号(A)
WEF2
有効期限(A)
ICカードa
(a)
MF
IEF1
鍵1(B)
IEF2
鍵2(B)
IEF3
鍵3(B)
IEF4
復号化用鍵(B)
IEF5
暗号化用鍵(B)
IEF6
暗号化用鍵(A)
WEF1
会員番号(B)
WEF2
有効期限(B)
ICカードb
(b)

【図５】

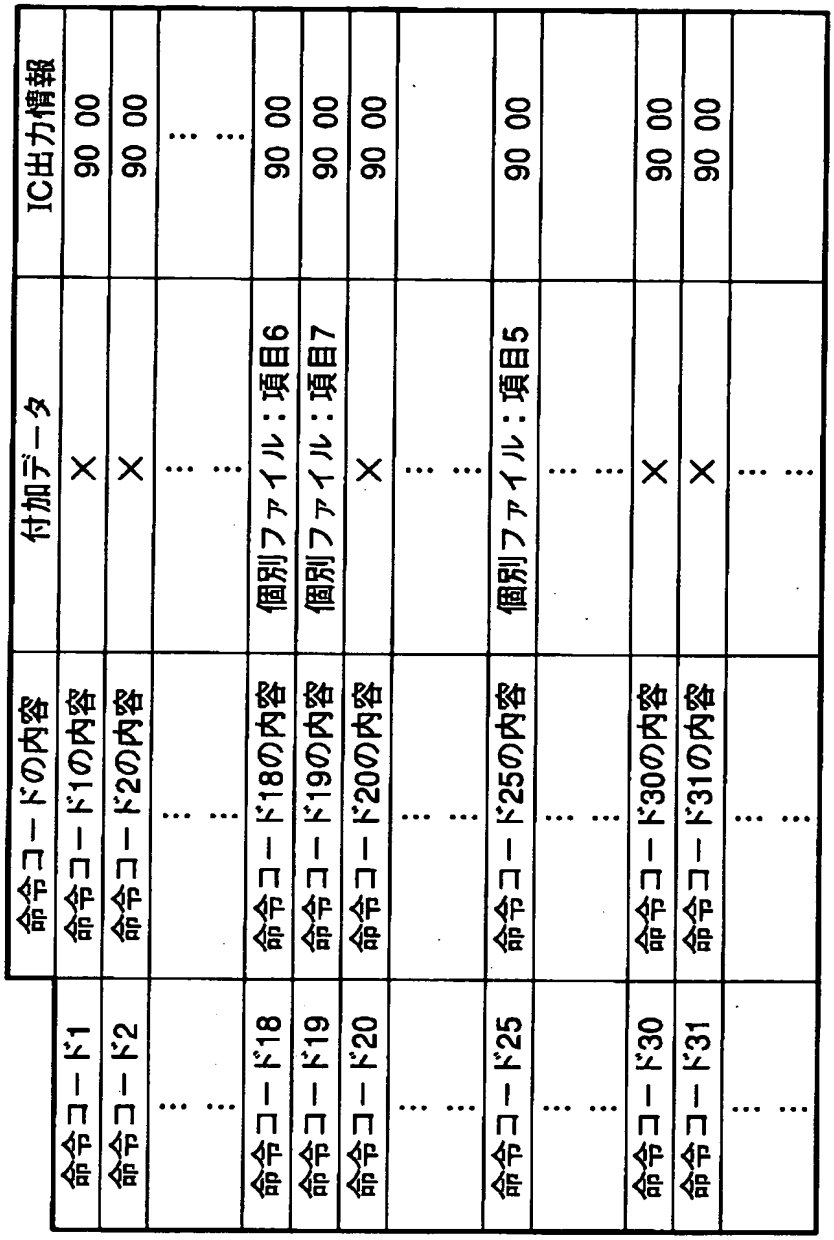

300
個人端末装置(A)
303
キーボード
HDD
302
301
演算部
電子データファイル1
(暗号化用鍵Aで暗号化)
F21
301b
メモリ
電子データファイル2
(暗号化用鍵Aで暗号化)
F22
301a
CPU
電子データファイル3
(暗号化用鍵Aで暗号化)
F23
ICカードa
カードリーダ・ライタA
304
ディスプレイ
100a
306
500
400
個人端末装置(B)
403
キーボード
HDD
402
401
演算部
電子データファイル1
(暗号化用鍵Bで暗号化)
F31
401a
CPU
電子データファイル2
(暗号化用鍵Bで暗号化)
F32
401b
メモリ
電子データファイル3
(暗号化用鍵Bで暗号化)
F33
ICカードb
カードリーダ・ライタB
404
ディスプレイ
100b
406

【図６】



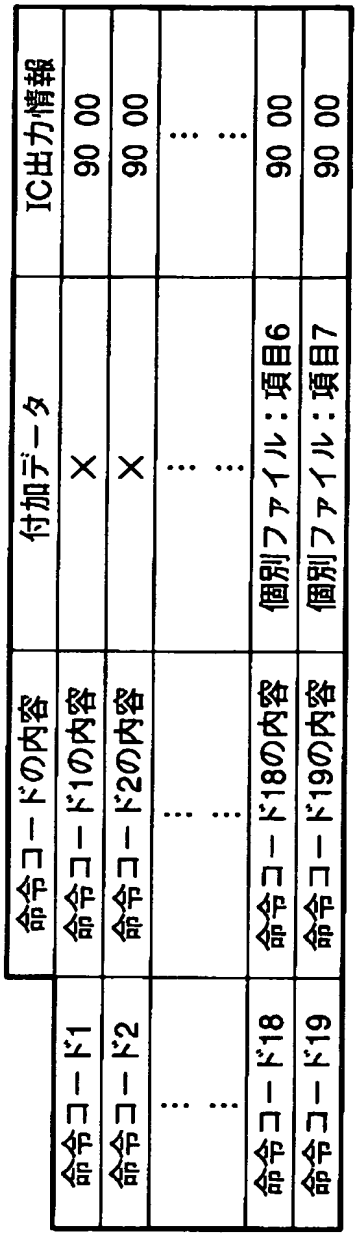
	項目1：漢字氏名	項目2：漢字住所	項目3：カナ名字	項目4：会員番号	項目5：有効期限	項目6：パスワード	項目7：鍵1
ﾚｺｰﾄﾞ#1	田中　太郎	練馬区	TANAKA	000007	2000.09	737c545a87	93 24..d8 88 AB
ﾚｺｰﾄﾞ#2	鈴木　次郎	江東区	SUZUKI	000014	2001.10	4787ea7184	d0 93..b2 cb 46
：	：	：	：	：	：	：	：
：	：	：	：	：	：	：	：
ﾚｺｰﾄﾞ#13	林　三郎	新宿区	HAYASHI	000157	2005.08	c8d7eb567f	82 6a..eb 0b 87
ﾚｺｰﾄﾞ#14	松本　四郎	杉並区	MATSUMOTO	000004	2002.07	8181fc35d8	49 83..6c 44 78
：	：	：	：	：	：	：	：
：	：	：	：	：	：	：	：
ﾚｺｰﾄﾞ#21	中村　五郎	品川区	NAKAMURA	002004	2000.12	eefaac5620	35 89..fb f9 90

【図７】



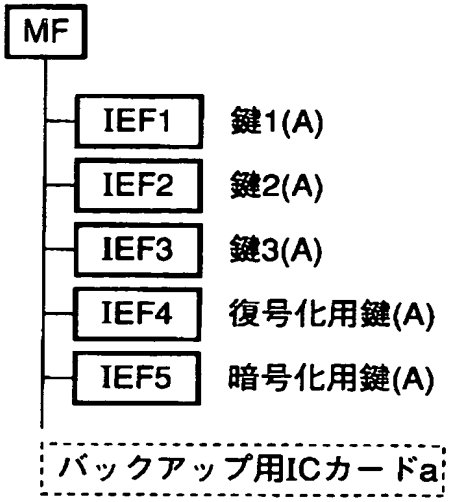
	命令コードの内容	付加データ	IC出力情報
命令コード1	命令コード1の内容	×	90 00
命令コード2	命令コード2の内容	×	90 00
… …	… …	… …	… …
命令コード18	命令コード18の内容	個別ファイル：項目6	90 00
命令コード19	命令コード19の内容	個別ファイル：項目7	90 00
命令コード20	命令コード20の内容	×	90 00
… …	… …	… …	
命令コード25	命令コード25の内容	個別ファイル：項目5	90 00
… …	… …	… …	
命令コード30	命令コード30の内容	×	90 00
命令コード31	命令コード31の内容	×	90 00
… …	… …	… …	

【図８】



	命令コードの内容	付加データ	IC出力情報
命令コード1	命令コード1の内容	×	90 00
命令コード2	命令コード2の内容	×	90 00
… …	… …	… …	… …
命令コード18	命令コード18の内容	個別ファイル：項目6	90 00
命令コード19	命令コード19の内容	個別ファイル：項目7	90 00

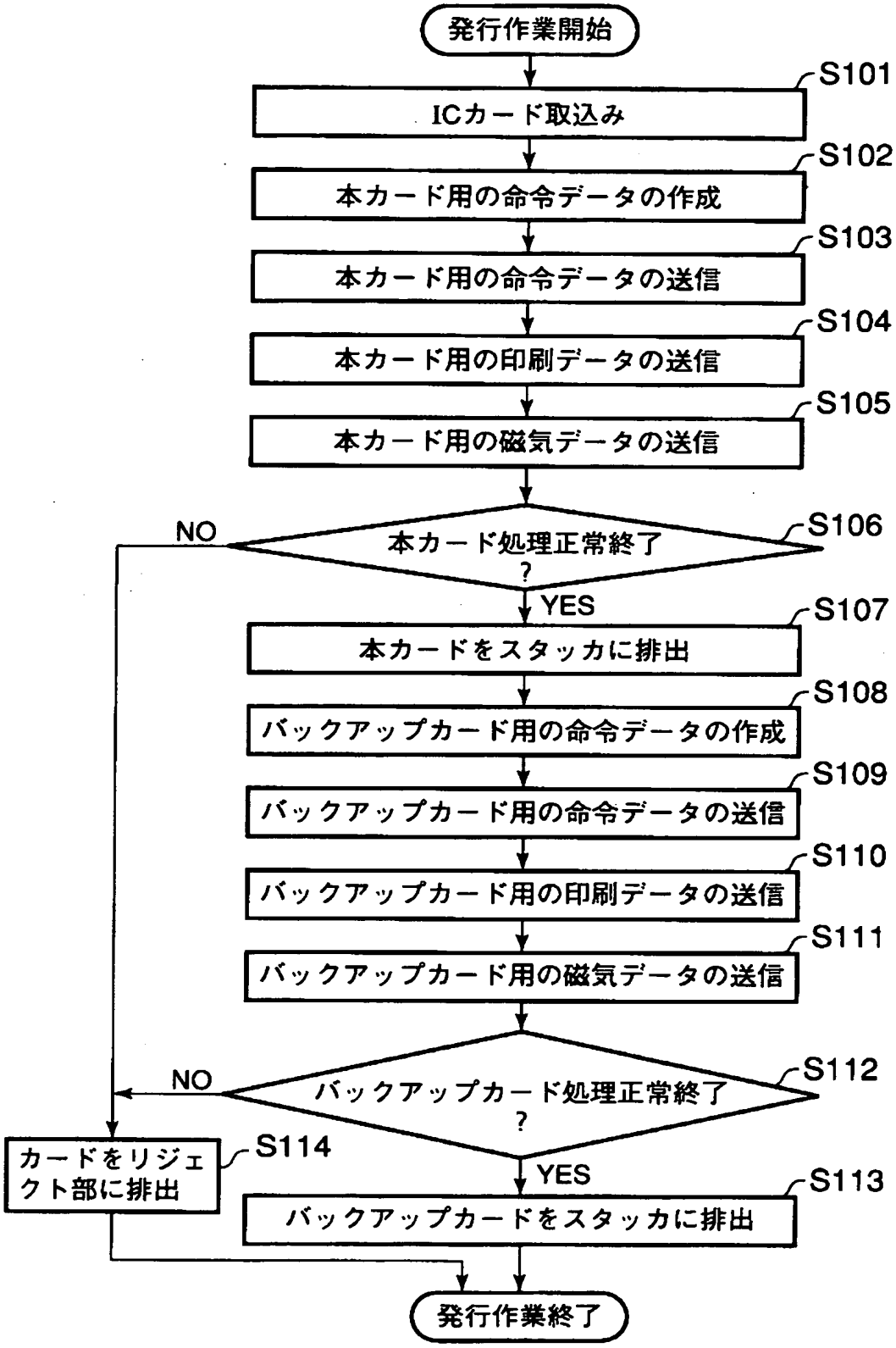
【図９】



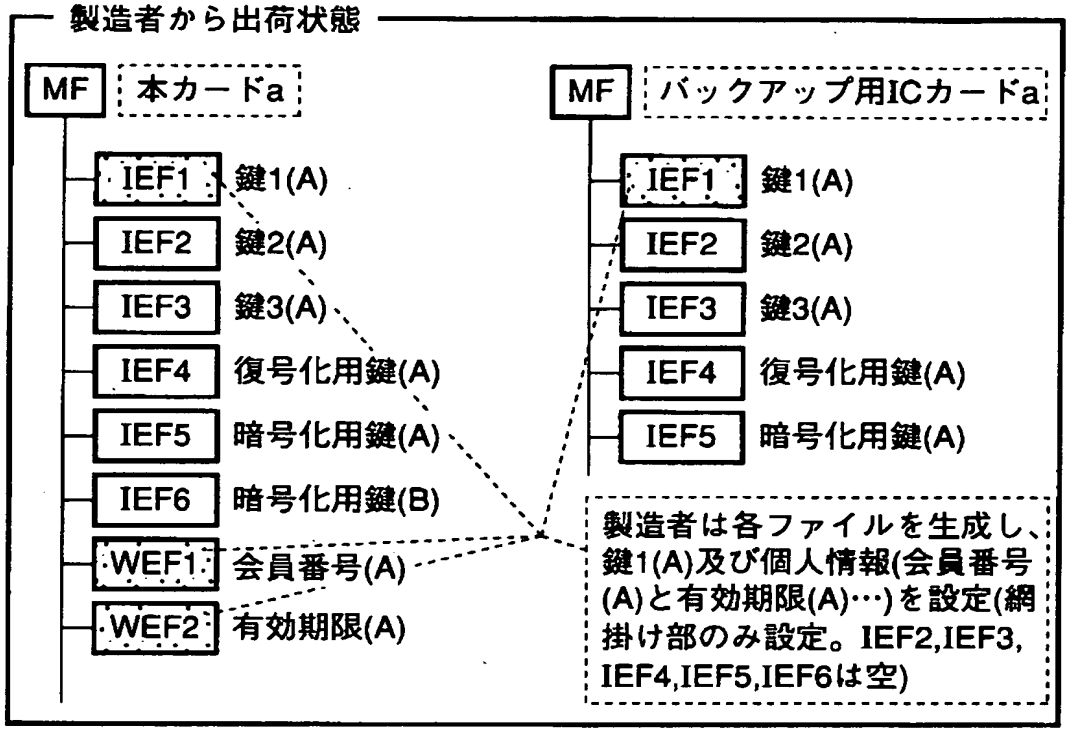
【図１０】

	付加データ
命令コード19の内容	49 83..6c 44 78

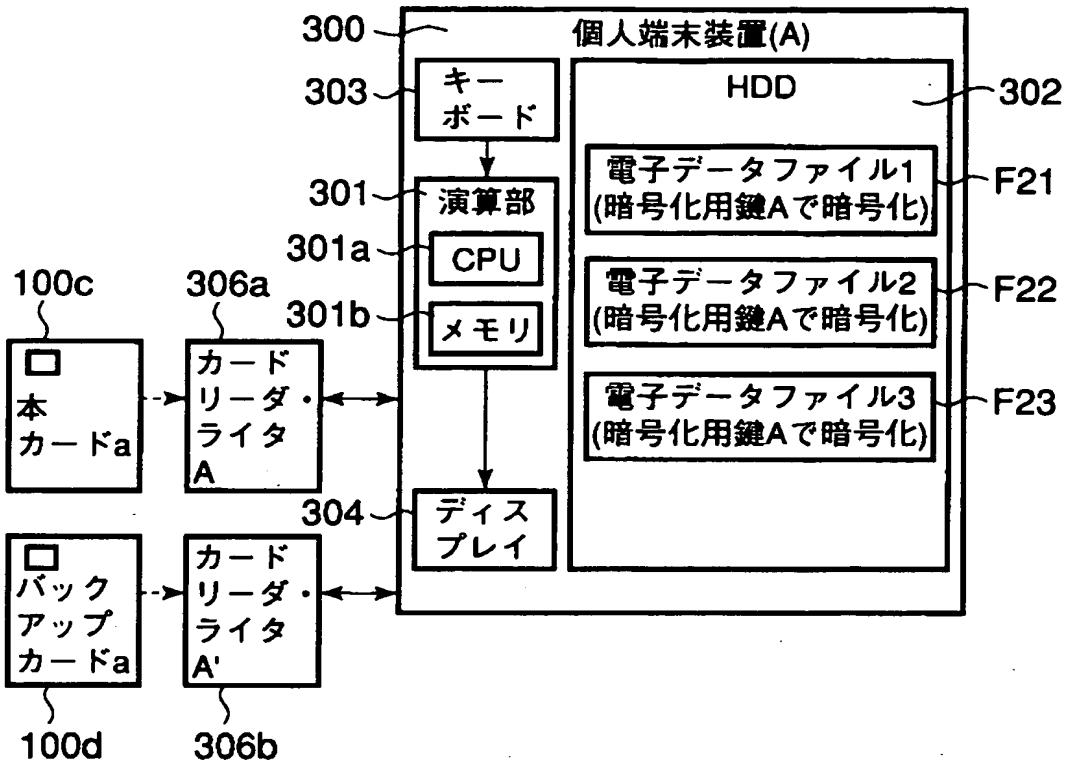
【図１１】


発行作業開始
S101
ICカード取込み
S102
本カード用の命令データの作成
S103
本カード用の命令データの送信
S104
本カード用の印刷データの送信
S105
本カード用の磁気データの送信
NO
本カード処理正常終了？
S106
YES
S107
本カードをスタッカに排出
S108
バックアップカード用の命令データの作成
S109
バックアップカード用の命令データの送信
S110
バックアップカード用の印刷データの送信
S111
バックアップカード用の磁気データの送信
NO
バックアップカード処理正常終了？
S112
YES
S113
バックアップカードをスタッカに排出
カードをリジェクト部に排出
S114
発行作業終了

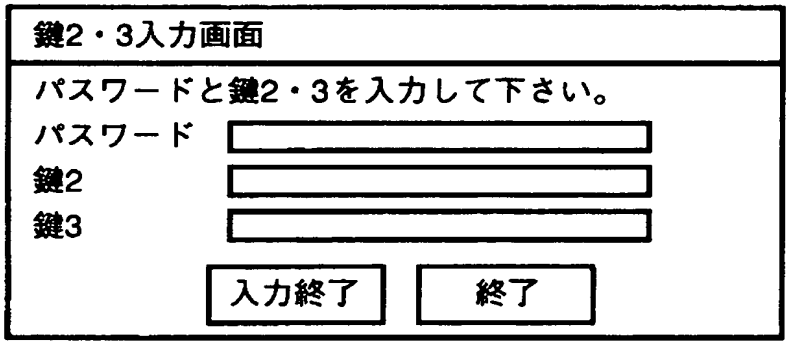
【図１２】


製造者から出荷状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
製造者は各ファイルを生成し、鍵1(A)及び個人情報(会員番号(A)と有効期限(A)…)を設定(網掛け部のみ設定。IEF2,IEF3,IEF4,IEF5,IEF6は空)

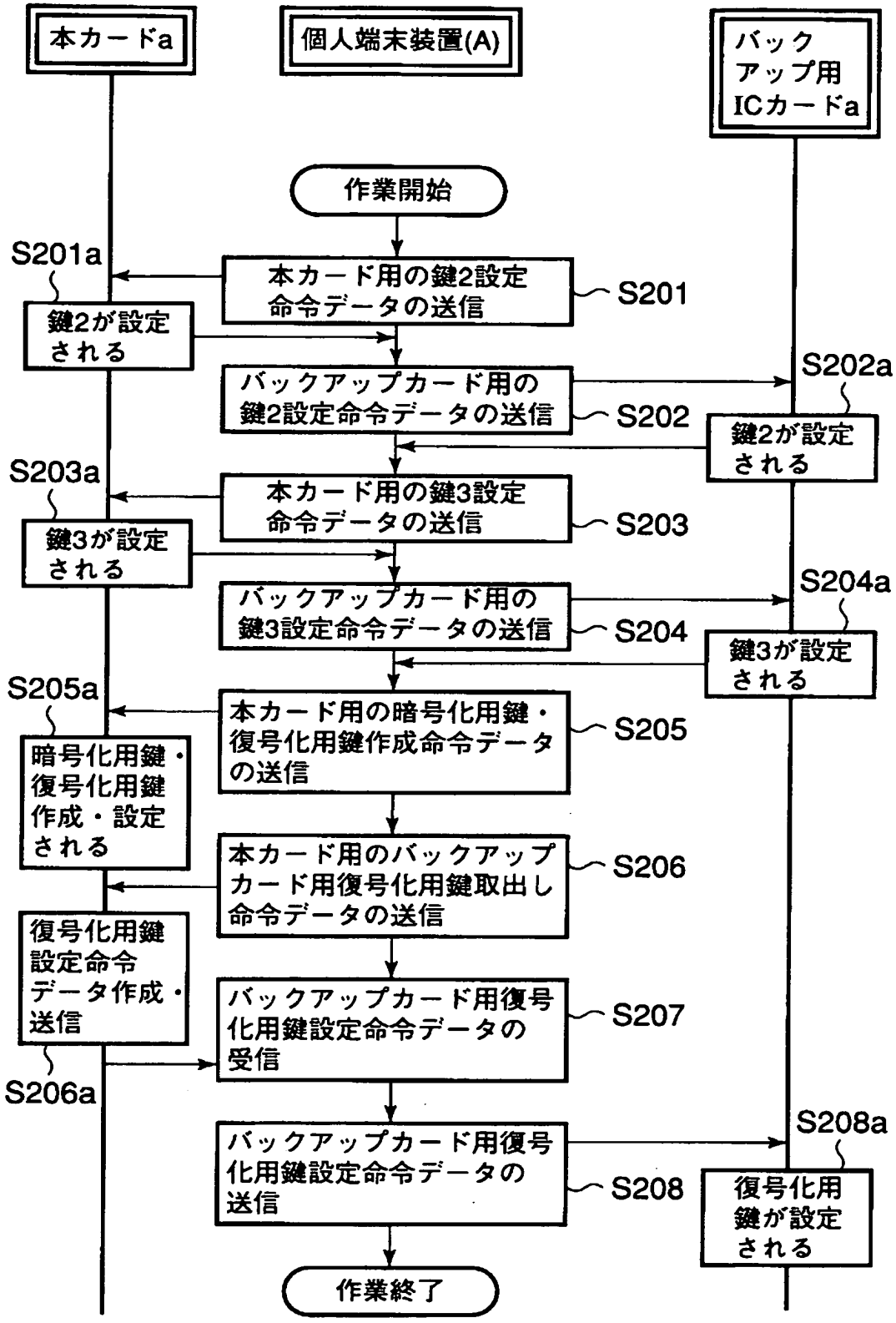
【図１３】


300
個人端末装置(A)
303
キーボード
HDD
302
301
演算部
301a
CPU
301b
メモリ
電子データファイル1
(暗号化用鍵Aで暗号化)
F21
電子データファイル2
(暗号化用鍵Aで暗号化)
F22
電子データファイル3
(暗号化用鍵Aで暗号化)
F23
304
ディスプレイ
100c
本カードa
306a
カードリーダ・ライタA
100d
バックアップカードa
306b
カードリーダ・ライタA'

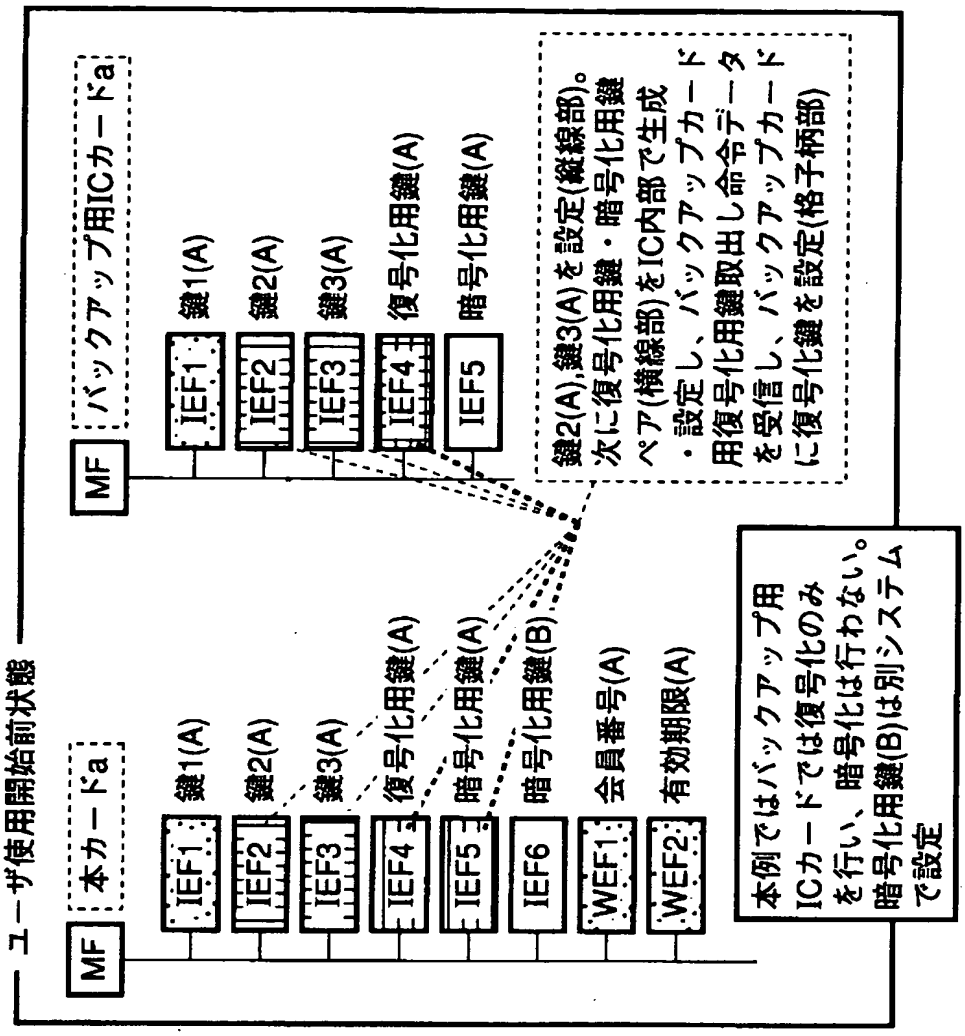
【図１４】


鍵2・3入力画面
パスワードと鍵2・3を入力して下さい。
パスワード
鍵2
鍵3
入力終了
終了

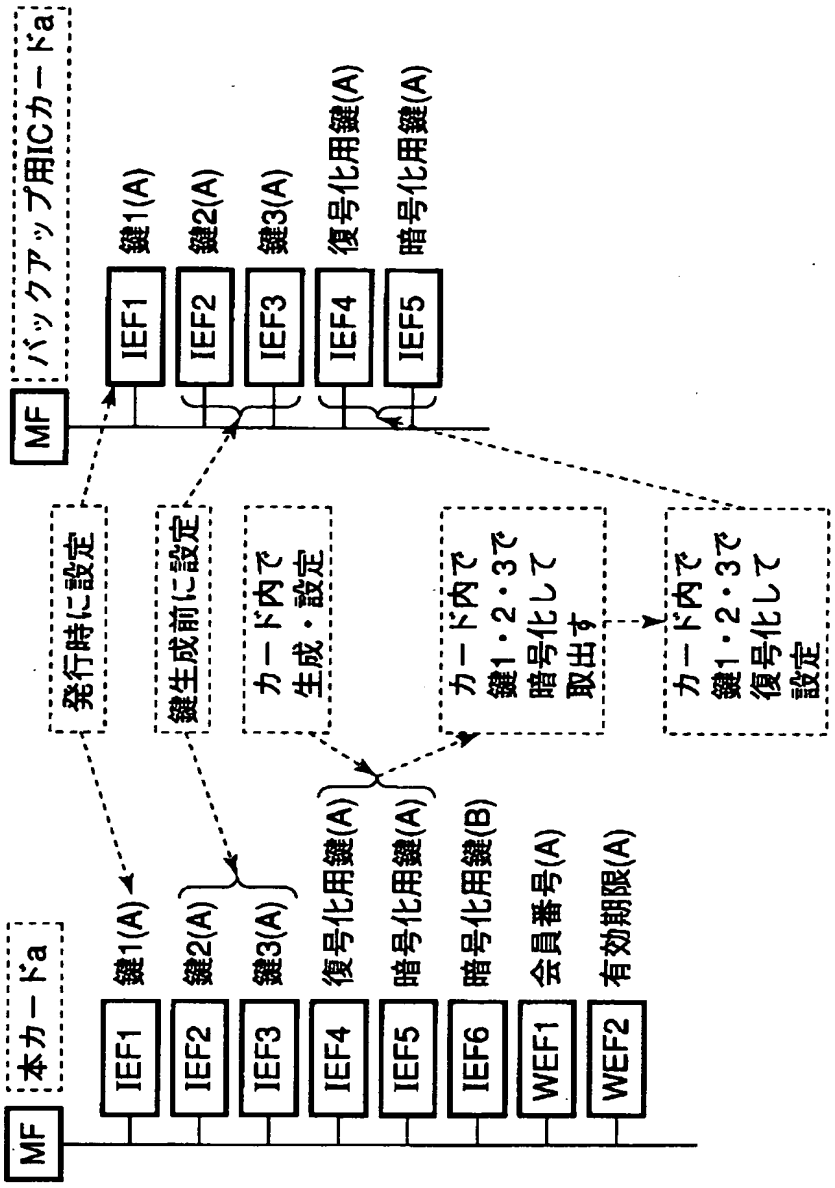
【図１５】


本カードa
個人端末装置(A)
バックアップ用ICカードa
作業開始
S201a
本カード用の鍵2設定命令データの送信
S201
鍵2が設定される
バックアップカード用の鍵2設定命令データの送信
S202
S202a
鍵2が設定される
S203a
本カード用の鍵3設定命令データの送信
S203
鍵3が設定される
バックアップカード用の鍵3設定命令データの送信
S204
S204a
鍵3が設定される
S205a
本カード用の暗号化用鍵・復号化用鍵作成命令データの送信
S205
暗号化用鍵・復号化用鍵作成・設定される
本カード用のバックアップカード用復号化用鍵取出し命令データの送信
S206
復号化用鍵設定命令データ作成・送信
バックアップカード用復号化用鍵設定命令データの受信
S207
S206a
バックアップカード用復号化用鍵設定命令データの送信
S208
S208a
復号化用鍵が設定される
作業終了

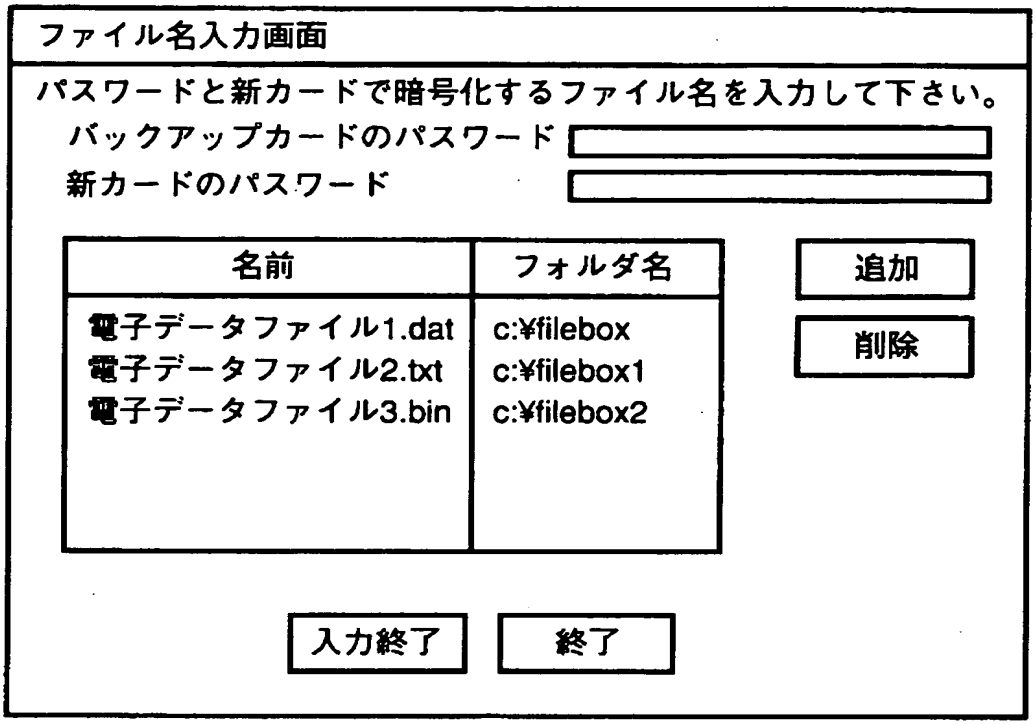
【図１６】


ユーザ使用開始前状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
鍵2(A),鍵3(A)を設定(縦線部)。
次に復号化用鍵・暗号化用鍵
ペア(横線部)をIC内部で生成
・設定し、バックアップカード
用復号化用鍵取出し命令データ
を受信し、バックアップカード
に復号化鍵を設定(格子柄部)
本例ではバックアップ用
ICカードでは復号化のみ
を行い、暗号化は行わない。
暗号化用鍵(B)は別システム
で設定

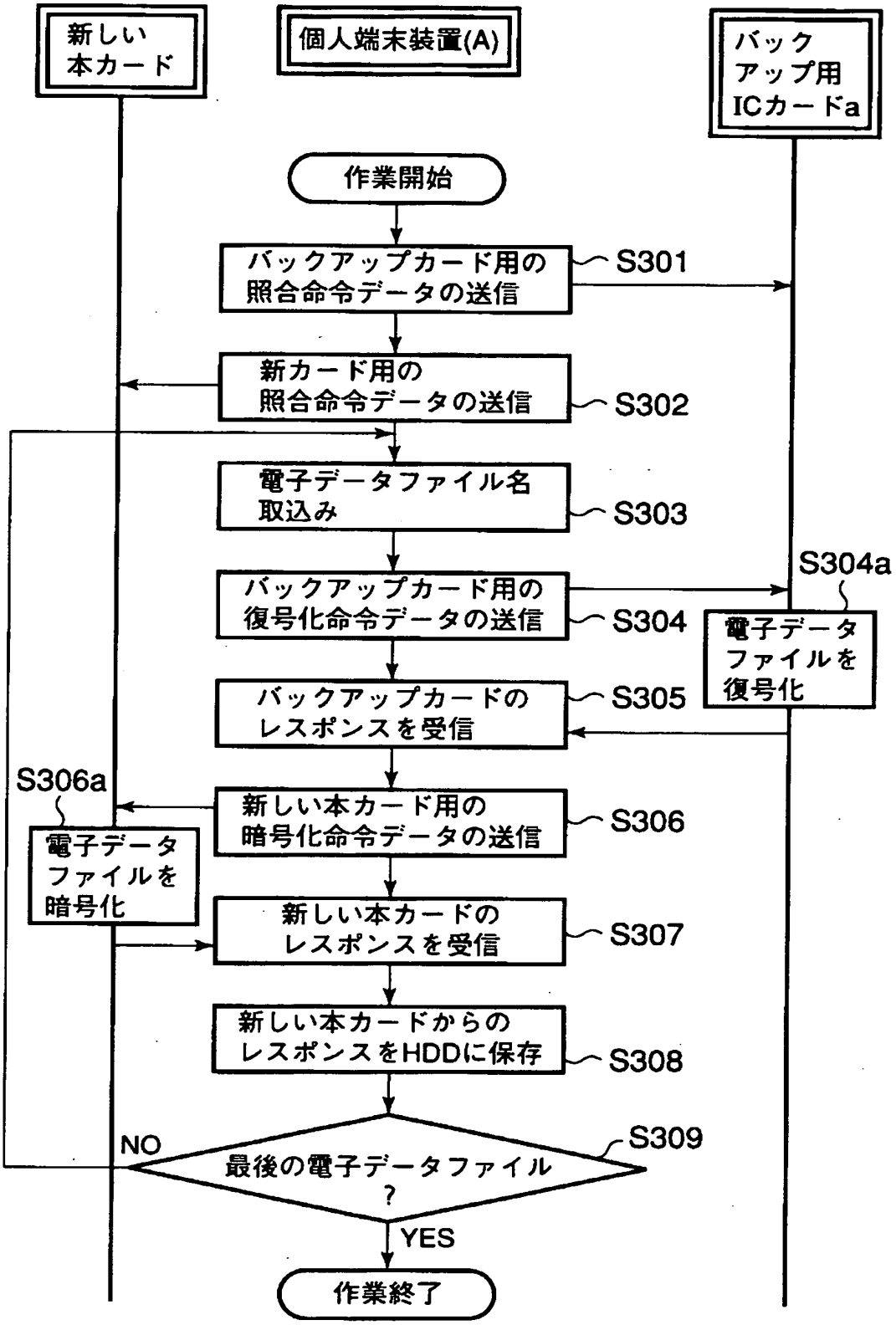
【図１７】


バックアップ用ICカードa
MF
IEF1
IEF2
IEF3
IEF4
IEF5
鍵1(A)
鍵2(A)
鍵3(A)
復号化用鍵(A)
暗号化用鍵(A)
発行時に設定
鍵生成前に設定
カード内で
生成・設定
カード内で
鍵1・2・3で
暗号化して
取出す
カード内で
鍵1・2・3で
復号化して
設定
本カードa
MF
IEF1
IEF2
IEF3
IEF4
IEF5
IEF6
WEF1
WEF2
鍵1(A)
鍵2(A)
鍵3(A)
復号化用鍵(A)
暗号化用鍵(A)
暗号化用鍵(B)
会員番号(A)
有効期限(A)

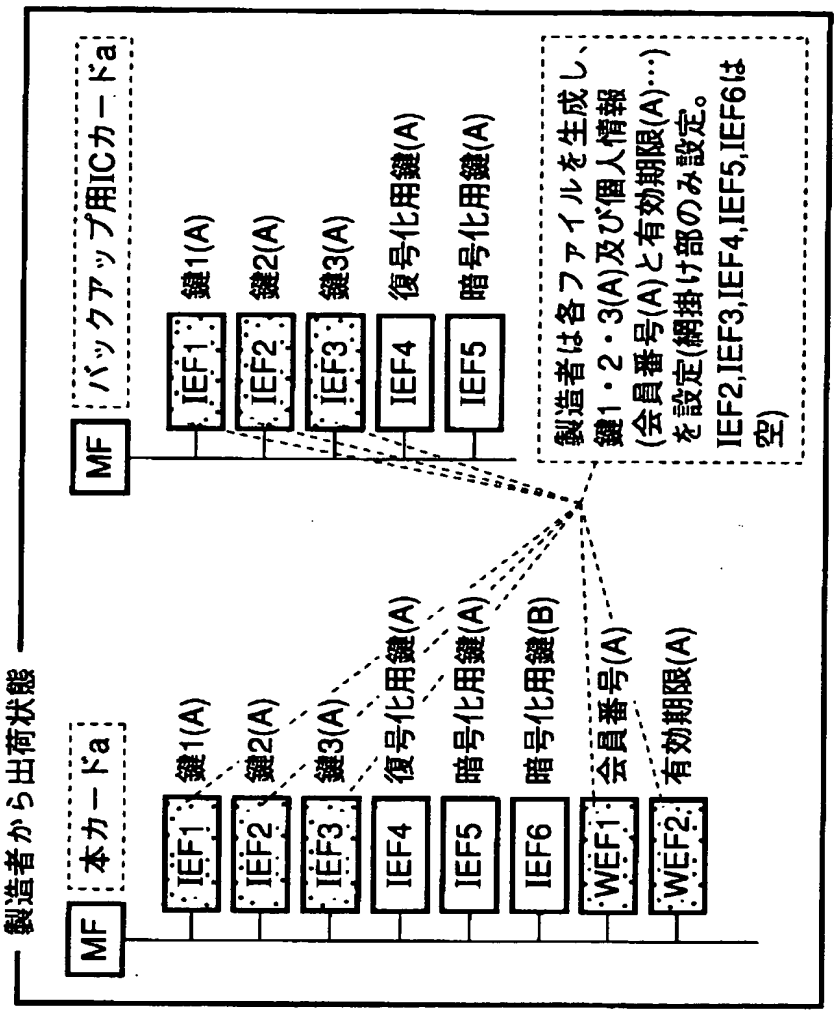
【図１８】


ファイル名入力画面
パスワードと新カードで暗号化するファイル名を入力して下さい。
バックアップカードのパスワード
新カードのパスワード
名前
フォルダ名
電子データファイル1.dat
電子データファイル2.txt
電子データファイル3.bin
c:¥filebox
c:¥filebox1
c:¥filebox2
追加
削除
入力終了
終了

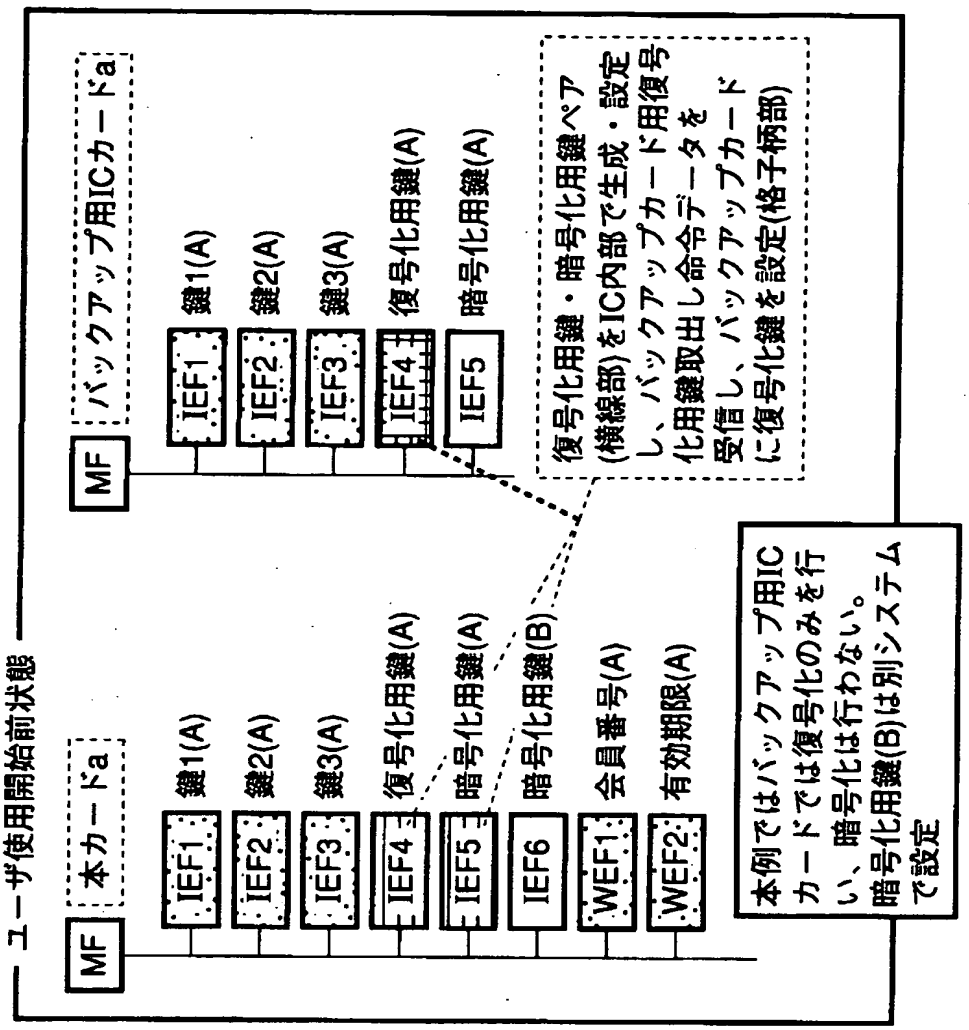
【図１９】


新しい本カード
個人端末装置(A)
バックアップ用ICカードa
作業開始
バックアップカード用の照合命令データの送信
S301
新カード用の照合命令データの送信
S302
電子データファイル名取込み
S303
バックアップカード用の復号化命令データの送信
S304
S304a
電子データファイルを復号化
バックアップカードのレスポンスを受信
S305
S306a
新しい本カード用の暗号化命令データの送信
S306
電子データファイルを暗号化
新しい本カードのレスポンスを受信
S307
新しい本カードからのレスポンスをHDDに保存
S308
NO
最後の電子データファイル？
S309
YES
作業終了

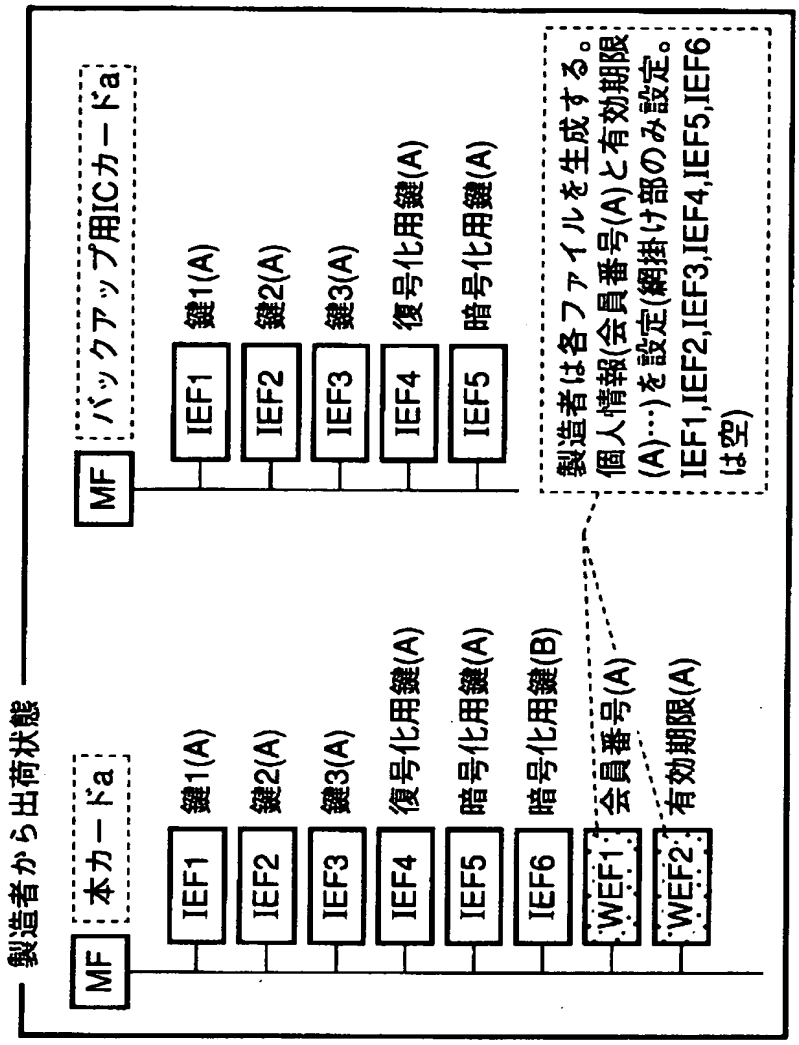
【図２０】


製造者から出荷状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
製造者は各ファイルを生成し、
鍵1・2・3(A)及び個人情報
(会員番号(A)と有効期限(A)…)
を設定(網掛け部のみ設定。
IEF2,IEF3,IEF4,IEF5,IEF6は
空)

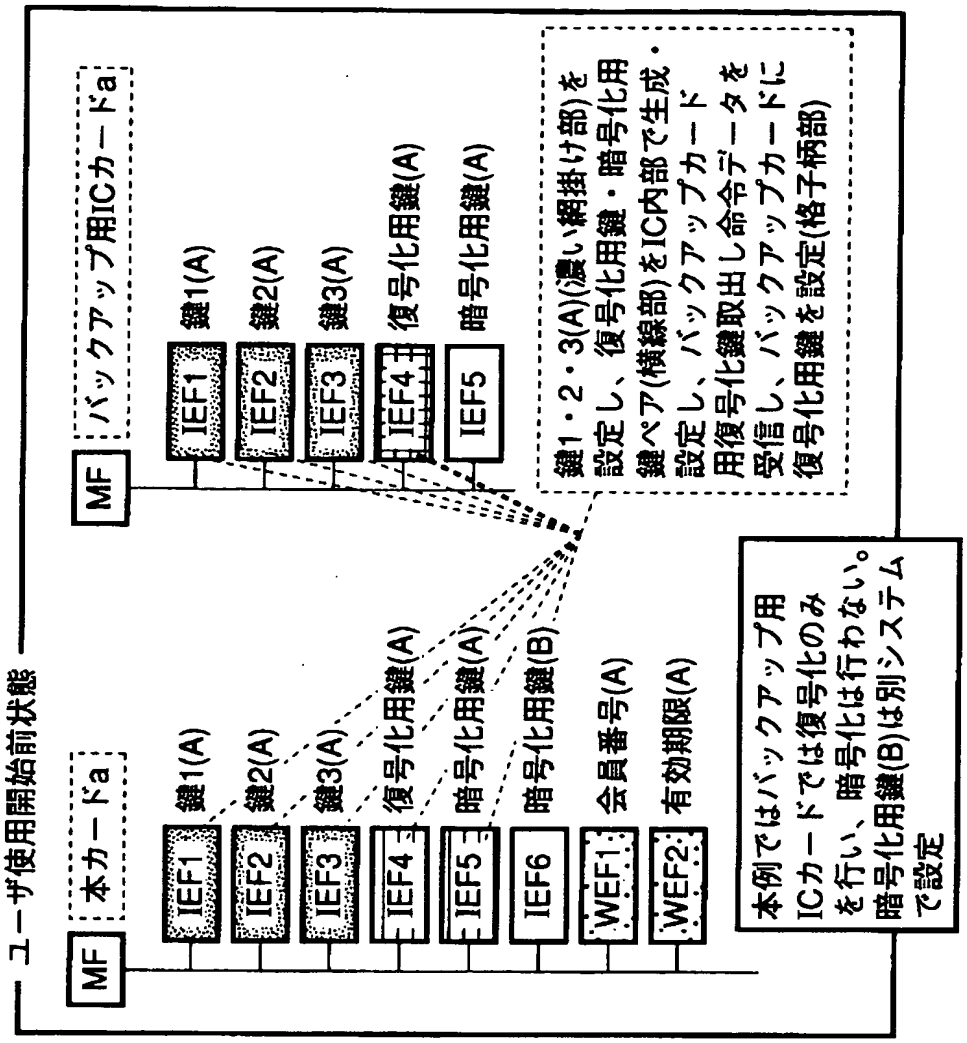
【図２１】


ユーザ使用開始前状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
復号化用鍵・暗号化用鍵ペア
(横線部)をIC内部で生成・設定
し、バックアップカード用復号
化用鍵取出し命令データを
受信し、バックアップカード
に復号化鍵を設定(格子柄部)
本例ではバックアップ用IC
カードでは復号化のみを行
い、暗号化は行わない。
暗号化用鍵(B)は別システム
で設定

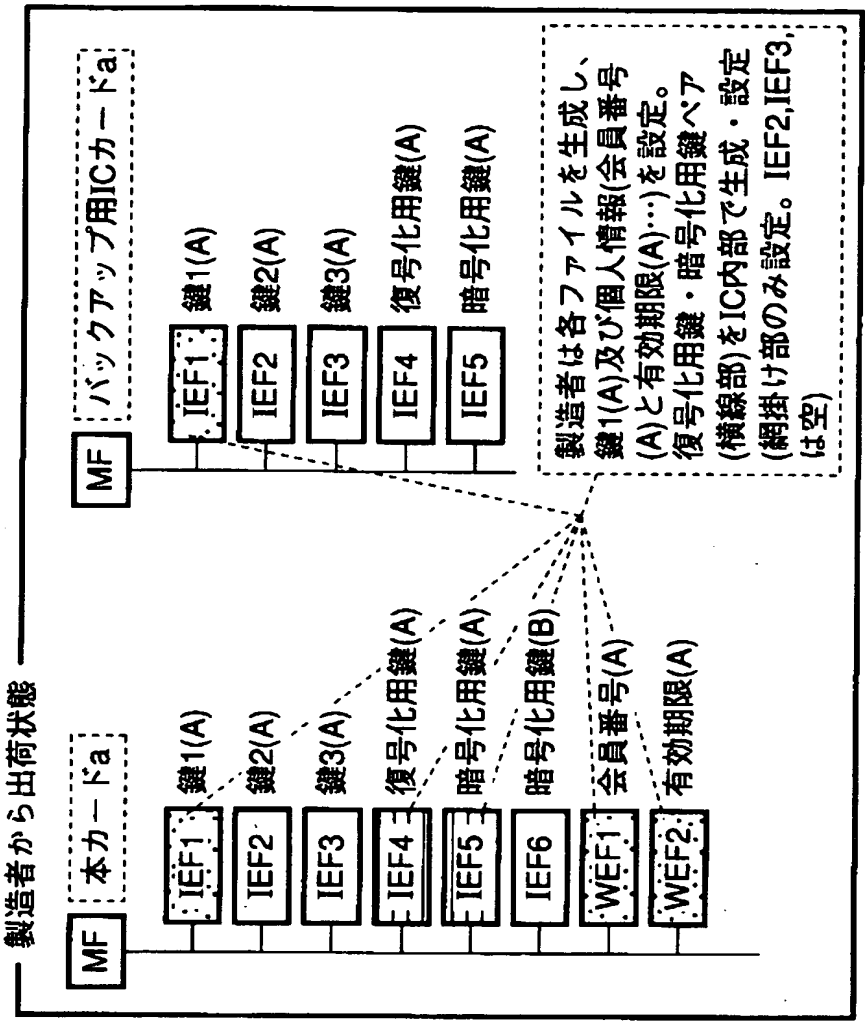
【図２２】


製造者から出荷状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
製造者は各ファイルを生成する。
個人情報(会員番号(A)と有効期限(A)…)を設定(網掛け部のみ設定。
IEF1,IEF2,IEF3,IEF4,IEF5,IEF6は空)

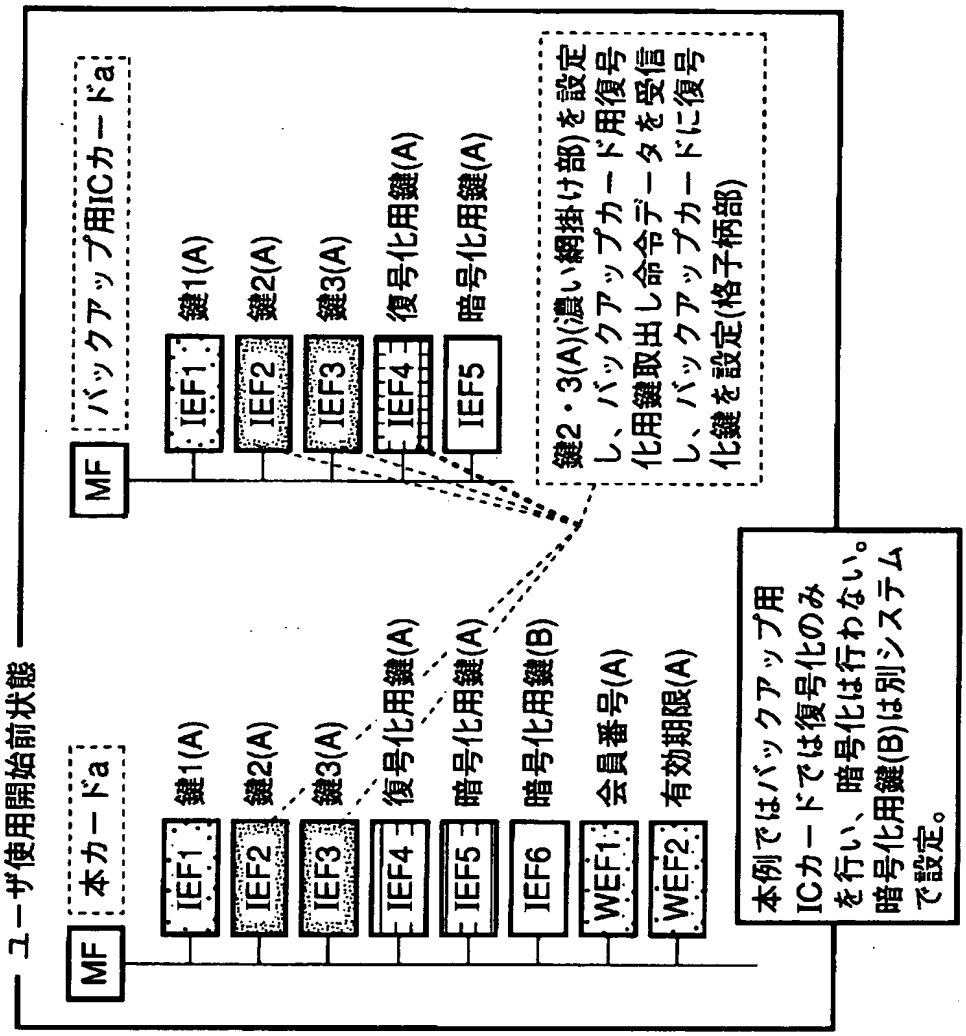
【図２３】


ユーザ使用開始前状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
本例ではバックアップ用
ICカードでは復号化のみ
を行い、暗号化は行わない。
暗号化用鍵(B)は別システム
で設定
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
鍵1・2・3(A)(濃い網掛け部)を
設定し、復号化用鍵・暗号化用
鍵ペア(横線部)をIC内部で生成・
設定し、バックアップカード
用復号化鍵取出し命令データを
受信し、バックアップカードに
復号化用鍵を設定(格子柄部)

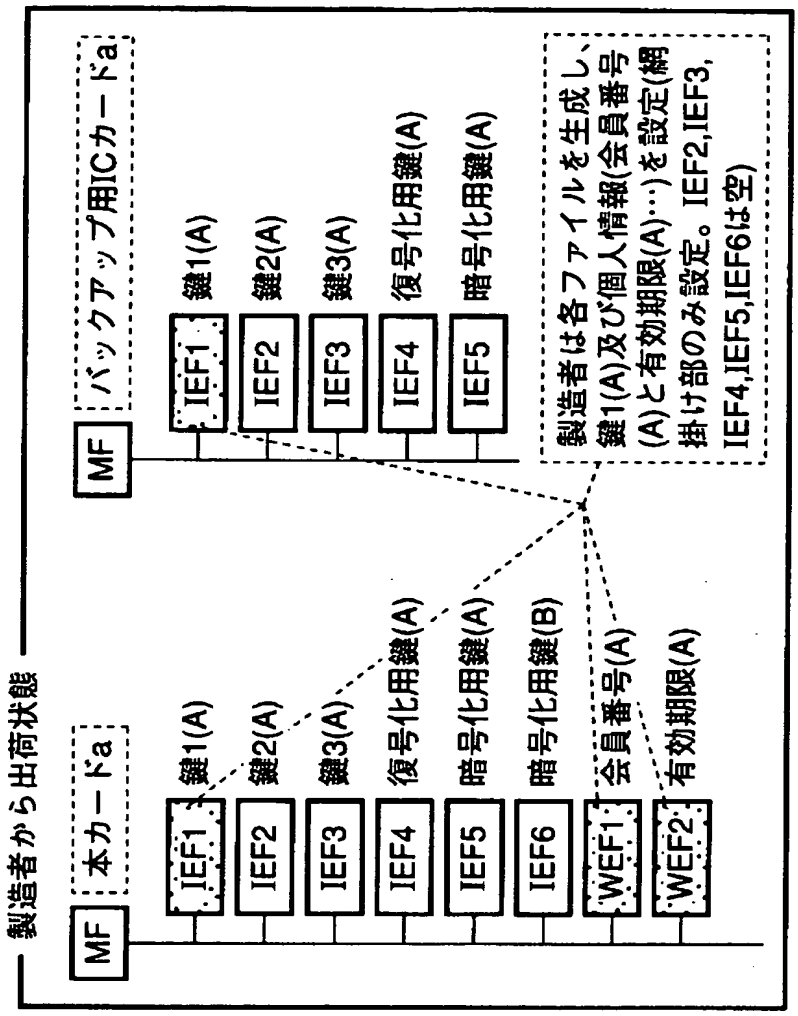
【図２４】


製造者から出荷状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
製造者は各ファイルを生成し、
鍵1(A)及び個人情報(会員番号
(A)と有効期限(A)…)を設定。
復号化用鍵・暗号化用鍵ペア
(横線部)をIC内部で生成・設定
(網掛け部のみ設定。IEF2,IEF3,
は空)

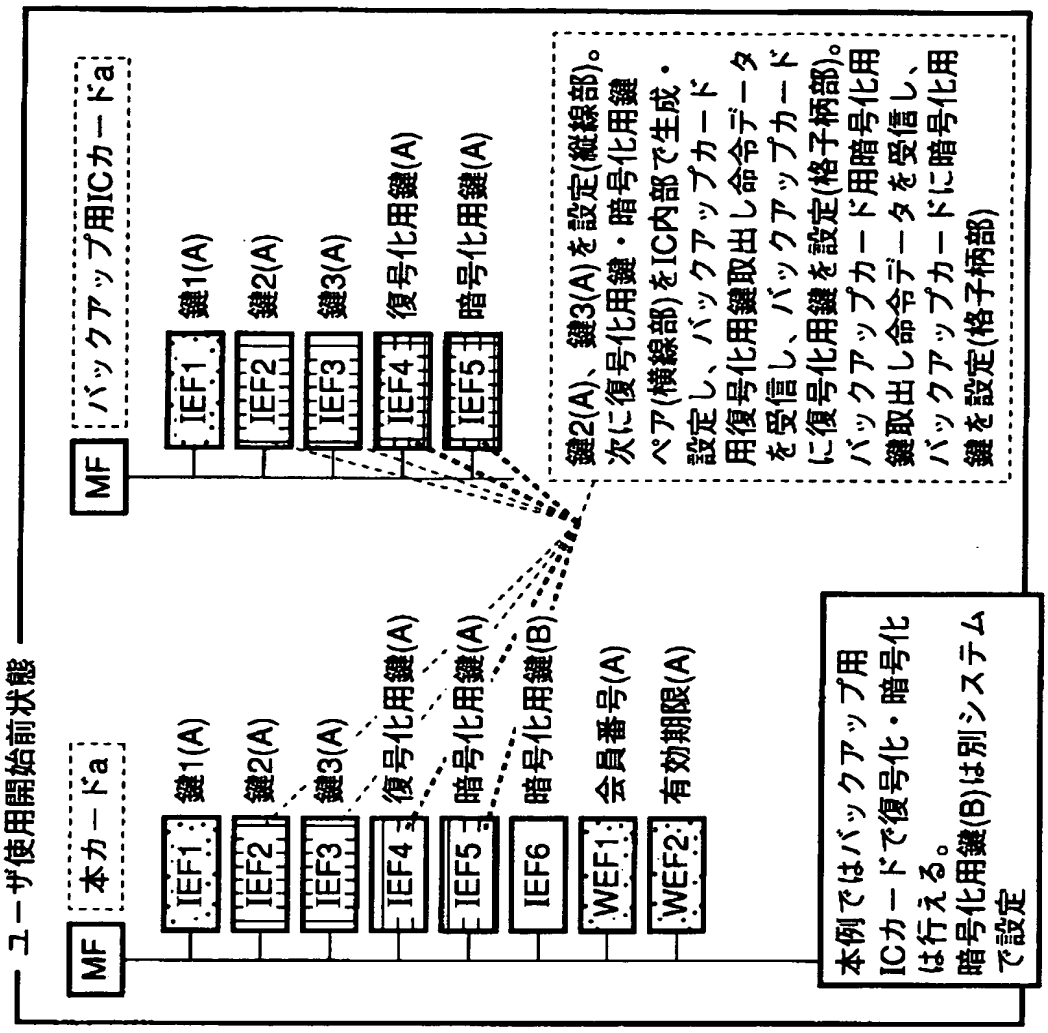
【図２５】


ユーザ使用開始前状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
鍵2・3(A)(濃い網掛け部)を設定し、バックアップカード用復号化用鍵取出し命令データを受信し、バックアップカードに復号化鍵を設定(格子柄部)
本例ではバックアップ用ICカードでは復号化のみを行い、暗号化は行わない。暗号化用鍵(B)は別システムで設定。

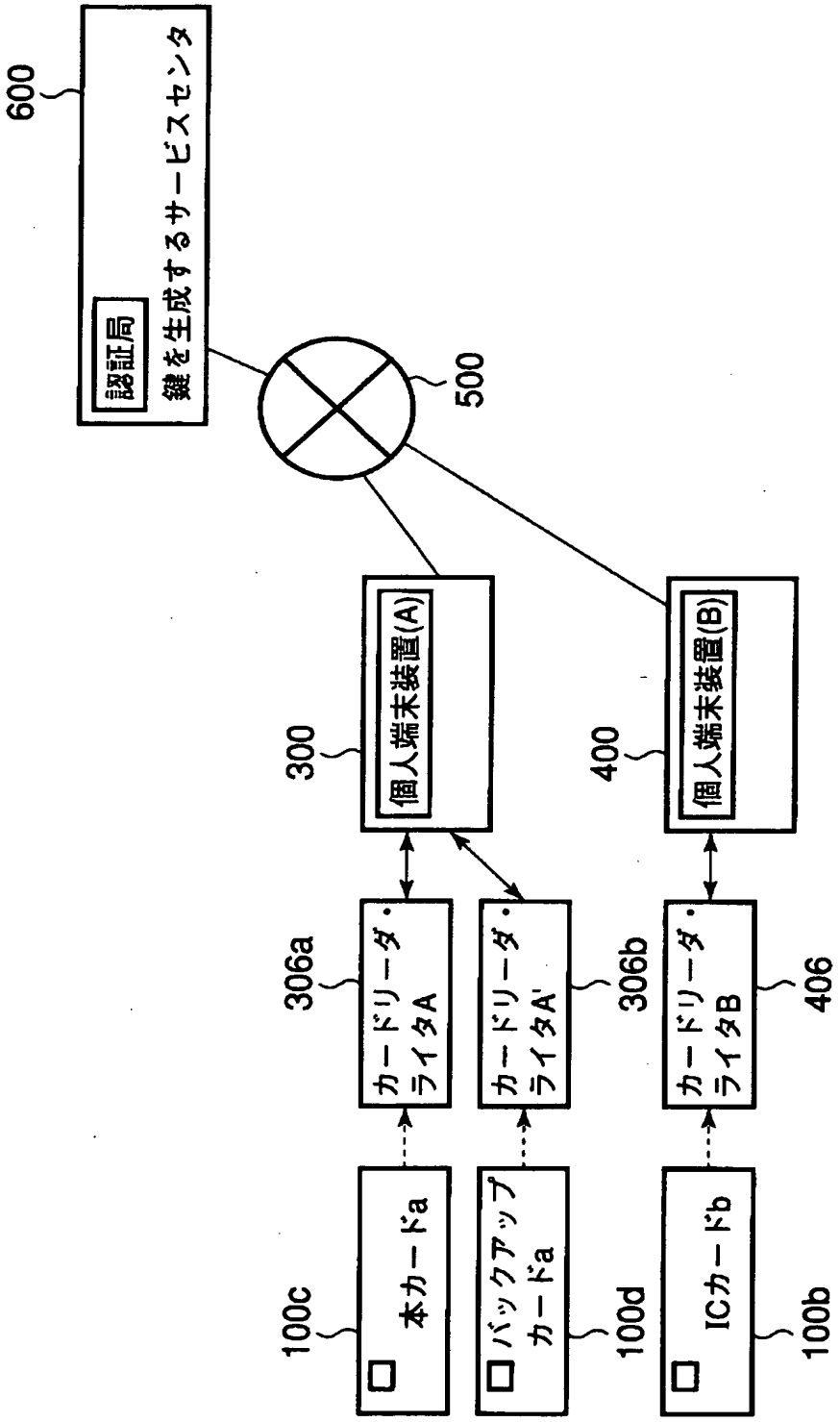
【図２６】


製造者から出荷状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
製造者は各ファイルを生成し、鍵1(A)及び個人情報(会員番号(A)と有効期限(A)…)を設定(網掛け部のみ設定。IEF2,IEF3,IEF4,IEF5,IEF6は空)

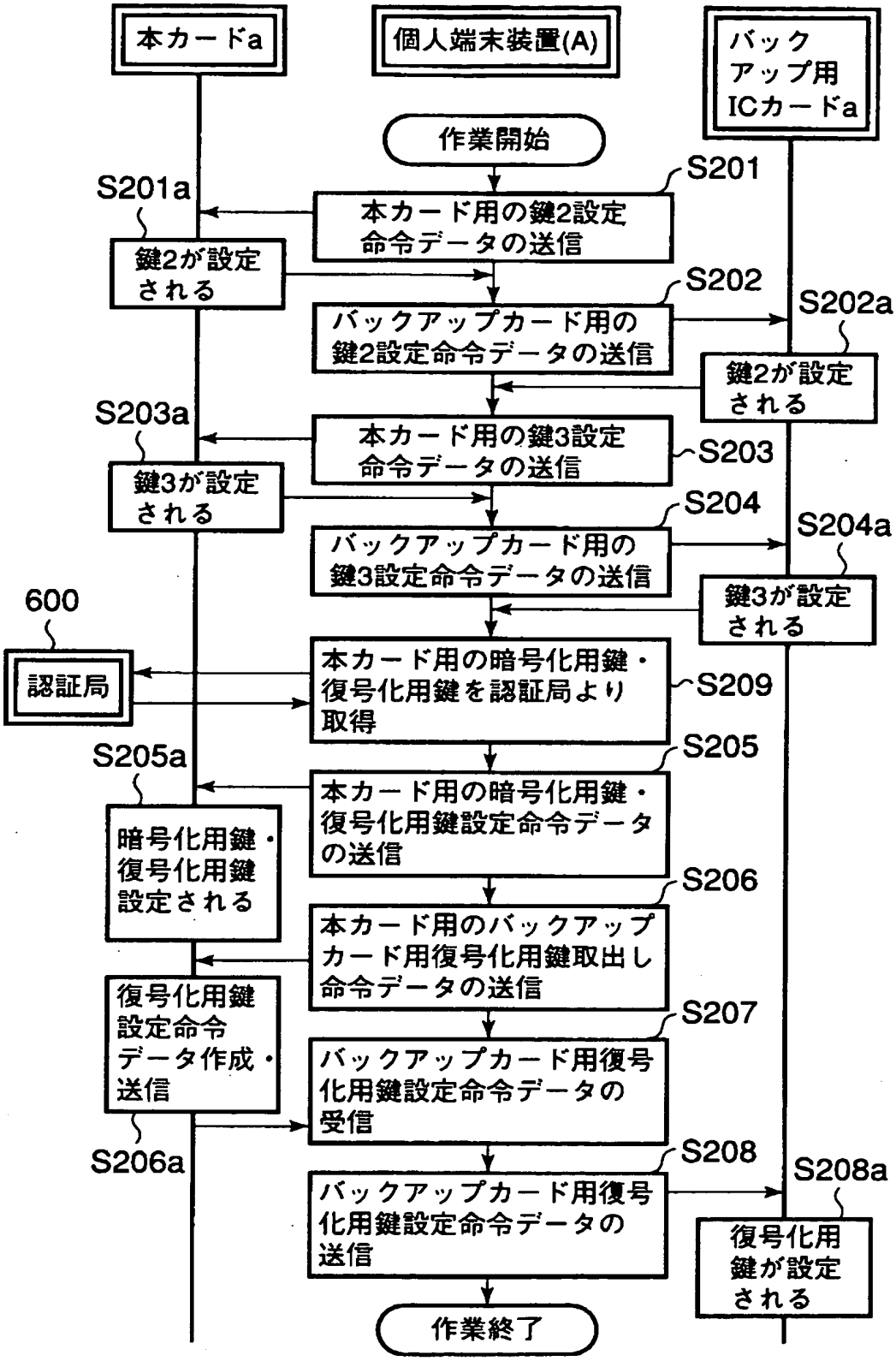
【図２７】


ユーザ使用開始前状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
鍵2(A)、鍵3(A)を設定(縦線部)。
次に復号化用鍵・暗号化用鍵
ペア(横線部)をIC内部で生成・
設定し、バックアップカード
用復号化用鍵取出し命令データ
を受信し、バックアップカード
に復号化用鍵を設定(格子柄部)。
バックアップカード用暗号化用
鍵取出し命令データを受信し、
バックアップカードに暗号化用
鍵を設定(格子柄部)
本例ではバックアップ用
ICカードで復号化・暗号化
は行える。
暗号化用鍵(B)は別システム
で設定

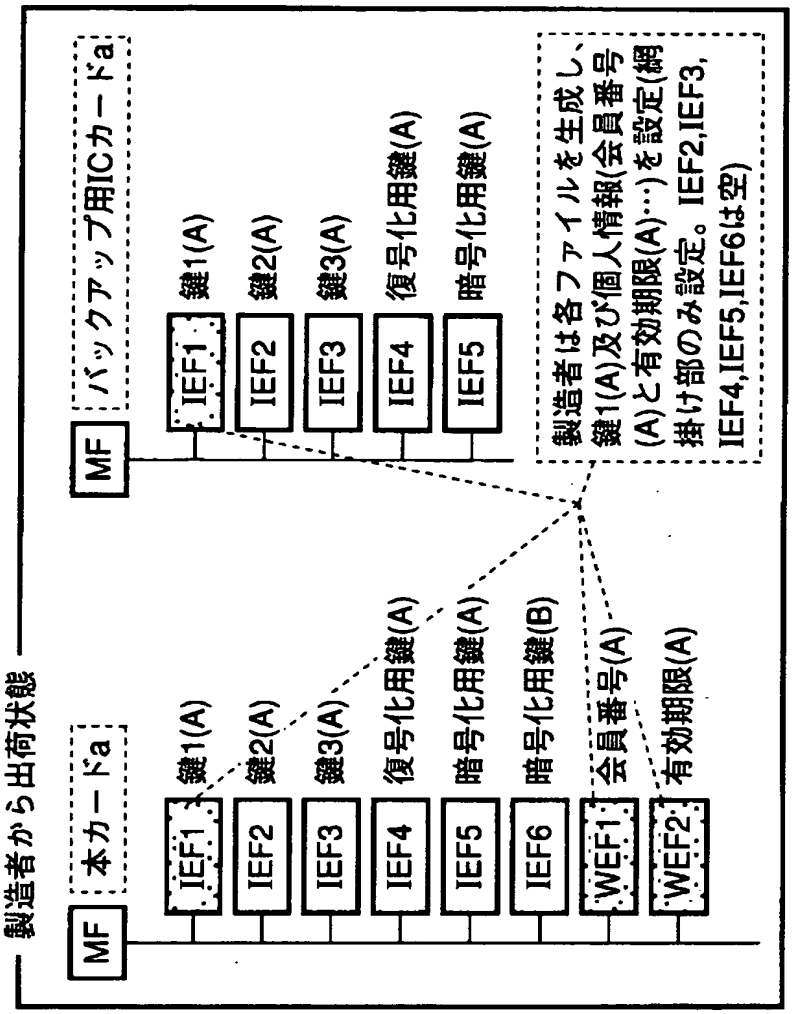
【図２８】


600
認証局
鍵を生成するサービスセンタ
500
300
個人端末装置(A)
400
個人端末装置(B)
306a
カードリーダ・ライタA
カードリーダ・ライタA'
306b
カードリーダ・ライタB
406
100c
本カードa
バックアップカードa
100d
ICカードb
100b

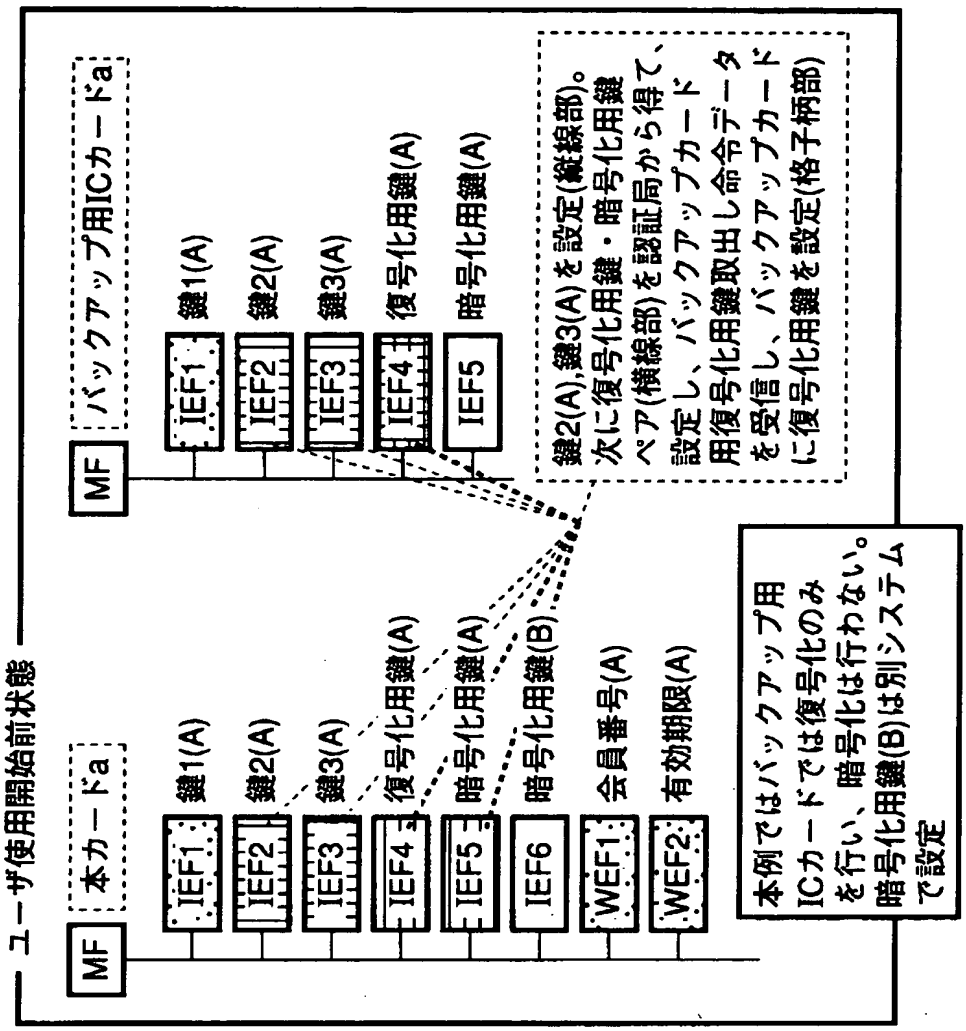
【図２９】


本カードa
個人端末装置(A)
バックアップ用ICカードa
作業開始
S201
本カード用の鍵2設定命令データの送信
S201a
鍵2が設定される
S202
バックアップカード用の鍵2設定命令データの送信
S202a
鍵2が設定される
S203a
鍵3が設定される
本カード用の鍵3設定命令データの送信
S203
S204
バックアップカード用の鍵3設定命令データの送信
S204a
鍵3が設定される
600
認証局
本カード用の暗号化用鍵・復号化用鍵を認証局より取得
S209
S205a
暗号化用鍵・復号化用鍵設定される
S205
本カード用の暗号化用鍵・復号化用鍵設定命令データの送信
S206
本カード用のバックアップカード用復号化用鍵取出し命令データの送信
復号化用鍵設定命令データ作成・送信
S207
バックアップカード用復号化用鍵設定命令データの受信
S206a
S208
バックアップカード用復号化用鍵設定命令データの送信
S208a
復号化用鍵が設定される
作業終了

【図３０】


製造者から出荷状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
製造者は各ファイルを生成し、鍵1(A)及び個人情報(会員番号(A)と有効期限(A)…)を設定(網掛け部のみ設定。IEF2,IEF3,IEF4,IEF5,IEF6は空)

【図３１】


ユーザ使用開始前状態
MF
本カードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
IEF6
暗号化用鍵(B)
WEF1
会員番号(A)
WEF2
有効期限(A)
MF
バックアップ用ICカードa
IEF1
鍵1(A)
IEF2
鍵2(A)
IEF3
鍵3(A)
IEF4
復号化用鍵(A)
IEF5
暗号化用鍵(A)
鍵2(A),鍵3(A)を設定(縦線部)。
次に復号化用鍵・暗号化用鍵
ペア(横線部)を認証局から得て、
設定し、バックアップカード
用復号化用鍵取出し命令データ
を受信し、バックアップカード
に復号化用鍵を設定(格子柄部)
本例ではバックアップ用
ICカードでは復号化のみ
を行い、暗号化は行わない。
暗号化用鍵(B)は別システム
で設定

【書類名】　　要約書

【要約】

【課題】内部に記憶された、データを暗号化あるいは復号化するための鍵を安全に外部へ取出すことのできるＩＣカードを提供する。

【解決手段】内部で生成あるいは外部から設定された、データを復号化するための復号化用鍵、データを暗号化するための暗号化用鍵を持つＩＣカードにおいて、ＩＣカード内の復号化用鍵、暗号化用鍵を外部へ取出すための鍵取出命令が入力された場合、該ＩＣカード内に設定された別の複数の鍵で復号化用鍵、暗号化用鍵を暗号化してから外部へ送出する。

【選択図】　　図１５

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　　神奈川県川崎市幸区堀川町７２番地
氏　名　　株式会社東芝